MINISTÈRE
CHARGÉ
DES TRANSPORTS

Liberté
Égalité
Fraternité

dgac direction générale de l'Aviation civile
DSAC

G-06-00

Système de gestion, conforme au règlement (UE) n°1321/2014

Direction de la sécurité de l'Aviation civile
Direction technique Navigabilité et Opérations
Édition n° 0
Version n° 0
Publiée le 20 décembre 2022

Gestion documentaire

Historique des révisions

Edition et version	Date	Modifications
Ed 0 v0	20 décembre 2022	Création.

Toute remarque ou proposition de modification portant sur un document peut être adressée à OSAC sur le site internet. Pour cela, le demandeur doit rechercher le document concerné sur la page Documentation Technique et sélectionner « Demander une modification » dans la colonne Actions.

Cette procédure est disponible en téléchargement sur le site internet :https://documentation.osac.aero/

Sommaire

1. OBJET 5
2. CONTEXTE ET RÉFÉRENCES RÉGLEMENTAIRES 5
3. ATTENDUS D'UN SYSTÈME DE GESTION (SG) 8
3.1. Généralités 8
3.1.1. Principes et fonctionnement 8
3.1.2. Taille et complexité de l'organisme 8
3.1.3. Intégration 9
3.2. Organisation et responsabilités 9
3.2.1. Généralités 9
3.2.2. Les postes clés 11
3.2.3. Les instances de gouvernance 14
3.3. Politique du système de gestion 15
3.3.1. Les objectifs 16
3.4. Gestion des risques 18
3.4.1. Généralités 18
3.4.2. Le processus de gestion des risques 25
3.4.2.1. L'identification des dangers 25
3.4.2.2. L'analyse des risques 28
3.4.2.3. L'évaluation des risques 31
3.4.2.4. Le traitement du risque 33
3.4.2.5. Comptes rendus d'événements en matière de sécurité 36
3.4.2.5.1. L'enquête interne 36
3.4.2.5.2. Les comptes rendus d'événements 37
3.4.2.6. Surveillance et mesure de la performance de sécurité 38
3.4.2.6.1. Généralités 38
3.4.2.6.2. La définition et le suivi des indicateurs 39
3.4.2.7. La gestion des changements 40
3.4.2.8. L'amélioration continue 41
3.4.2.9. L'emergency response plan (ERP) 41
3.5. Maintien des compétences des personnels 42
3.5.1. La promotion de la sécurité 42
3.5.1.1. La formation 42
3.5.1.2. La communication 43
3.6. Documentation 43
3.7. Contrôle de la conformité 44
3.7.1. La fonction de surveillance de la conformité, une approche en deux phases 44
3.7.2. Exigences 45
3.7.3. Modalités 46
3.7.4. Auditeurs et autres acteurs de la surveillance de la conformité 46
3.7.5. Programme de surveillance interne 46
3.7.6. Système de retour d'informations 47
3.8. Exigences supplémentaires – contrats et contrats de sous-traitance 48
4. ANNEXE 49
4.1. Les composantes d'une organisation : schémas généraux 49

4.2. Les dysfonctionnements et la maîtrise des risques.....50
4.3. Management et pilotage 51
4.4. Notions sur le concept de Facteurs Organisationnels et Humains (FOH) 53
4.5. La culture de sécurité 53

1. OBJET

L'objet du présent guide est d'expliciter les attendus relatifs à la mise en œuvre d'un système de gestion (SG) et de décrire des principes de base permettant d'y satisfaire. Les moyens mis en œuvre par les organismes pour satisfaire à ces principes peuvent varier.

Les références réglementaires citées dans le présent guide proviennent de la Partie-CAMO du règlement (UE) n°1321/2014 et de ses moyens de conformité.
Il peut être possible de démontrer sa conformité aux règles par d'autres moyens, en développant un moyen alternatif de conformité conformément à l'exigence CAMO.A.120.

Conformément à l'exigence CAMO.A.200(d), pour les transporteurs aériens titulaires d'une licence de transport aérien octroyée conformément au règlement (CE) n°1008/2008, le système de gestion de l'organisme agréé Partie-CAMO doit faire partie intégrante du système de gestion du transporteur aérien. Par conséquent, dans la forme et dans les grands principes, ce guide vise l'homogénéité avec le guide DSAC intitulé « système de gestion des exploitants (ORG-SV) ».

2. CONTEXTE ET RÉFÉRENCES RÉGLEMENTAIRES

Le transport aérien est une industrie à risque ce qui entraine une exigence de sécurité élevée.
Il y a donc création de règles qui limitent l'exposition au risque par l'encadrement de pratiques (fiabilité dans la conception, modes opératoires, conditions de travail ou d'exploitation, formations…).
Dans cette logique, la sécurité est assurée par la bonne application des règles et la supervision (interne-externe) de cette bonne application. Ici apparaissent les notions de conformité réglementaire et de surveillance de la conformité.
Ce type d'encadrement des pratiques se fait à un niveau global. Les règles sont générales et sont les mêmes pour tous.

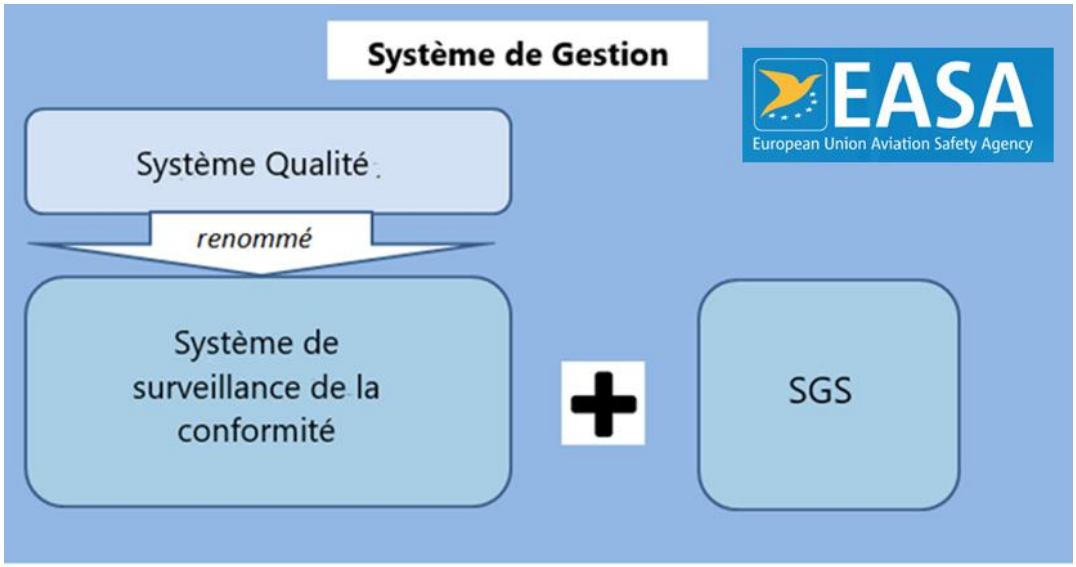
Mais il existe un niveau local : l'organisation (atelier, exploitant, gestionnaire de navigabilité…).
Cette dernière est caractérisée par :

- des activités et des pratiques particulières ;
- une culture particulière ;
- une adaptation fréquente à des situations imprévues.

Pour assurer la continuité de l'exigence de sécurité dans ce niveau local, une gestion structurée de cette sécurité s'impose à travers le système de gestion de la sécurité qui prend en compte l'assurance du respect des normes d'une part et la gestion des risques locaux d'autre part.

Il peut être compris comme un ensemble de personnes, de ressources, de politiques, de procédures, qui interagissent de manière organisée, dans le but de prévenir les accidents et de réduire la gravité des dommages.

Le modèle de système de gestion défini par l'EASA est :



Le système de gestion correspond à l'agrégation et la consolidation des composantes conformité et sécurité de l'organisme préexistantes.

L'exigence européenne de mise en œuvre d'un système de gestion pour les organismes agréés existe déjà dans de nombreux domaines (opérations aériennes conformément au règlement (UE) n° 965/2012 par exemple). Cette exigence, au niveau européen, concerne notamment les organismes impliqués dans la gestion du maintien de la navigabilité, de la réalisation de l'entretien et de la production des aéronefs et de leurs éléments. En effet, ces organismes agréés doivent disposer d'un Système de Gestion conforme, entre autres, respectivement aux exigences du CAMO.A.200, du 145.A.200 et à compter du 07/03/2024 du 21.A.139.

Ainsi, ce guide sera complété au fur et à mesure de l'entrée en vigueur des exigences relatives à l'instauration des systèmes de gestion dans les autres types d'organismes cités. Il peut néanmoins déjà être considéré comme modèle d'amélioration.

En parallèle des exigences réglementaires européennes, en France, l'arrêté du 22/12/2008 relatif à la mise en œuvre des Systèmes de Gestion de la Sécurité (SGS) et son instruction associée s'appliquent aux organismes français agréés Partie-145.

Le présent guide **(G-06-00)** cohabite donc avec le guide pratique sur les systèmes de gestion de la sécurité pour les activités de maintien de la navigabilité **(P-50-11),** qui reste applicable pour les organismes agréés Partie-145 dont la gestion de la sécurité relève encore de l'arrêté du 22/12/2008 cité ci-dessus, à savoir ceux n'ayant pas terminé leur période de transition dans le cadre de la prise en compte du règlement (UE) 2021/1963 (cf. BI 2022/01).

Pour les organismes CAMO ayant mis en œuvre un SGS suivant l'arrêté du 22/12/2008, un système de correspondance entre les exigences EASA, l'arrêté de 2008 et le guide OACI est proposé dans le tableau suivant afin de les aider dans leur démarche de conversion.

	Exigences EASA		Manuel SGS OACI	Arrêté du 22/12/2008
	Catégories d'exigence	Applicable CAMO		
GÉNÉRALITÉS	Système de gestion (complexité)	**CAMO.A.200 (b)**		
	Système de gestion (intégration possible du SG)	**CAMO.A.200 (c)**		
	Système de gestion (intégration obligatoire du SG AOC)	**CAMO.A.200 (d)**		Article 4 (c)
HARMONISATION DES SG	Système de gestion (Harmonisation du SG même groupement économique)	**CAMO.A.200 (e)**		
ORGANISATION ET RESPONSABILITÉS	Système de gestion (Définitions des fonctions et des responsabilités. Responsabilité directe du Dirigeant Responsable en matière de sécurité)	**CAMO.A.200 (a)(1)**	1.2 Obligation de rendre compte et responsabilités en matière de sécurité 1.3 Nomination du personnel clé chargé de la sécurité	Article 5 (1) (2)
POLITIQUE DU SG	Système de gestion (Politique de sécurité et objectifs)	**CAMO.A.200 (a)(2)**	1.1 Engagement de la direction	Article 4 (a) (1)
GESTION DES RISQUES	Système de gestion (Identification des dangers et gestion des risques)	**CAMO.A.200 (a)(3)**	2.1 Identification des dangers 2.2 Évaluation et atténuation des risques de sécurité 1.4 Coordination de la planification des interventions d'urgence 3.1 Suivi et mesure de la performance de sécurité 3.2 La gestion du changement 3.3 Amélioration continue du SGS	Article 4 (a) (2) (3)
	Compte rendu d'événements Dispositif interne de compte rendu en matière de sécurité	**CAMO.A.160 CAMO.A.202** Règlement (UE**) 376/2014** Règlement d'exécution (UE) **2015/1018**		Article 4 (b)
MAINTIEN DES COMPÉTENCES DES PERSONNELS	Système de gestion (Maintien de personnel formé et compétent)	**CAMO.A.200 (a)(4)**	4.1 Formation et sensibilisation 4.2 Communication en matière de sécurité	Article 4 (a) (4)
DOCUMENTATION	Système de gestion (Documentation des principaux processus du système de gestion)	**CAMO.A.200 (a)(5)**	1.5 Documentation relative au SGS	Article 6
CONTROLE DE LA CONFORMITÉ	Système de gestion (Fonction de contrôle de la conformité, retour d'information vers le dirigeant responsable, mise en œuvre effective des actions correctives)	**CAMO.A.200 (a)(6)**		
	Système de gestion (Constatations de l'autorité	**CAMO.A.150**		
EXIGENCES SUPPLÉMENTAIRES	Système de gestion (Toutes exigences complémentaires	**CAMO.A.200 (a)(7)**		
	Système de gestion (Contrats et contrats de sous-traitance)	**CAMO.A.205**		

3. ATTENDUS D'UN SYSTÈME DE GESTION (SG)

3.1. Généralités

Références réglementaires	
CAMO.A.200	Système de gestion
GM au CAMO.A.200	Management system

3.1.1. Principes et fonctionnement

Le système de gestion de l'EASA regroupe les éléments du système de gestion de l'OACI définis à l'appendice 2 de l'annexe 19 avec la surveillance de la conformité réglementaire.

Cette approche vise à intégrer la gestion de la sécurité dans la stratégie globale des organismes de manière à définir des objectifs prioritaires pertinents, à les atteindre à l'aide d'actions et assurer ainsi la sécurité du maintien de la navigabilité et de l'exploitation.

L'efficacité de la gestion de la sécurité dépend en grande partie du degré d'engagement de tous les niveaux de la hiérarchie afin de créer un environnement de travail qui optimise la performance humaine, la coopération entre les personnels des organisations, la détection des dysfonctionnements et leur traitement.

Ainsi la réglementation relative au système de gestion requiert les points essentiels en matière de gestion de la sécurité :

a) La définition des responsabilités ;
b) L'établissement d'une politique de sécurité et des objectifs de sécurité associés ;
c) La mise en œuvre des procédures de compte rendu de sécurité conformes aux principes de la culture juste ;
d) L'identification des risques de sécurité relatifs à l'activité avec :
   - la définition de mesures pour atténuer les risques ;
   - la vérification de l'efficacité des mesures prises pour atténuer les risques ;
e) La surveillance de la conformité ;
f) Le maintien d'un personnel formé et informé en ce qui concerne notamment les problématiques de sécurité majeures ;
g) La documentation de tous les processus clés du système de gestion.

Par rapport aux exigences réglementaires précédemment applicables et relatives au système qualité de l'organisme, les nouveaux éléments introduits avec la mise en place d'un système de gestion sont notamment ceux visés aux points b) à d).

3.1.2. Taille et complexité de l'organisme

Références réglementaires	
CAMO.A.200(b)	Système de gestion (Taille et complexité)

Même si les exigences réglementaires sont les mêmes pour tous les organismes, chaque organisme déploie des méthodes de travail adaptées à sa taille, ainsi qu'à la nature et à la complexité de ses activités.

Exemple de critères de complexité pouvant être pris en compte :

Nombre de sites dont dispose l'organisme, nombre d'aéronefs en gestion, nombre de types d'aéronefs en gestion, nombre de sous-traitant(s) de tâches de gestion de navigabilité…

3.1.3. Intégration

Références réglementaires	
CAMO.A.200(c)	Système de gestion (Taille et complexité)
CAMO.A.200(d)	Système de gestion (intégration obligatoire)
CAMO.A.200(e)	Système de gestion (Harmonisation SG même groupement économique)
AMC1 M.A.201 (ea)*	Responsabilities

Lorsque l'organisme est titulaire d'un ou de plusieurs agréments qui relèvent du champ d'application du règlement (UE) 2018/1139, le système de gestion peut être intégré à ceux déjà requis.

Pour les transporteurs aériens titulaires d'une licence octroyée conformément au règlement (CE) n°1008/2008, le système de gestion prévu à la présente annexe fait partie intégrante du système de gestion du transporteur aérien.

Lorsque, conformément au point M.A.201 ea bis) de l'annexe I (partie M), un contrat est conclu entre un CAMO et des exploitants faisant partie d'un même groupement économique de transporteurs aériens, le CAMO doit faire en sorte que son système de gestion soit harmonisé avec les systèmes de gestion des exploitants faisant partie de ce groupement économique.

Selon l'AMC1 M.A.201(ea), l'harmonisation prend en compte les points suivants :

- des réunions pour partager les résultats et les conclusions de chaque Safety Review Board (SRB commun ou réunions dédiées), en présence des dirigeants responsables, des Safety Manager et de tout autre personnel désigné approprié.
- des échanges réguliers concernant les résultats et les conclusions de la fonction gestion de la conformité (et de la surveillance des autorités compétentes), en présence des dirigeants responsables, des Compliance Monitoring Manager et de tout autre personnel désigné approprié.
- une politique de sécurité commune ou cohérente (et les indicateurs de sécurité associés).
- des processus/procédures communs ou cohérents sur les sujets suivants :
  - Identification des dangers et gestion des risques associés.
  - Audit/enquête interne.
  - Surveillance et mesure de la performance de sécurité.
  - Gestion des changements.
  - Amélioration continue.
  - Emergency Response Plan.

3.2. Organisation et responsabilités

3.2.1. Généralités

Note : Les points réglementaires suivis du symbole (*) n'entrent pas dans le périmètre strict du SG. Ils sont cités à des fins d'explications.

Références réglementaires	
CAMO.A.200 (a)(1)	Système de gestion
AMC1 CAMO.A.200 (a)(1)	Management system
GM2 CAMO.A.200 (a)(1)	Management system
CAMO.A.305(a)(3)(4)(5)(b)(2)*	Exigences en matière de personnel
CAMO.A.130(a)(2)(3)*	Modifications de l'organisme

Les responsabilités sont clairement définies au sein de l'organisme avec la désignation des fonctions suivantes :

- un dirigeant responsable – DR ;
- une personne ou un groupe de personnes à qui incombe la responsabilité de s'assurer que l'organisme respecte toujours les exigences applicables en matière de gestion du maintien de la navigabilité : le Responsable Désigné - RDE (dans les cas transporteurs aériens titulaires d'une licence octroyée conformément au règlement (CE) n°1008/2008) ou une personne ou un groupe de personne dans les autres cas ;
- une personne ou un groupe de personnes à qui incombe la responsabilité de gérer la fonction de contrôle de la conformité : le Responsable de la Surveillance de la Conformité – RSC ;

- une personne ou un groupe de personnes à qui incombe la responsabilité de gérer l'élaboration, l'administration et le maintien de processus efficaces de gestion de la sécurité dans le cadre du système de gestion : Le Responsable de la Gestion de la Sécurité – RGS.

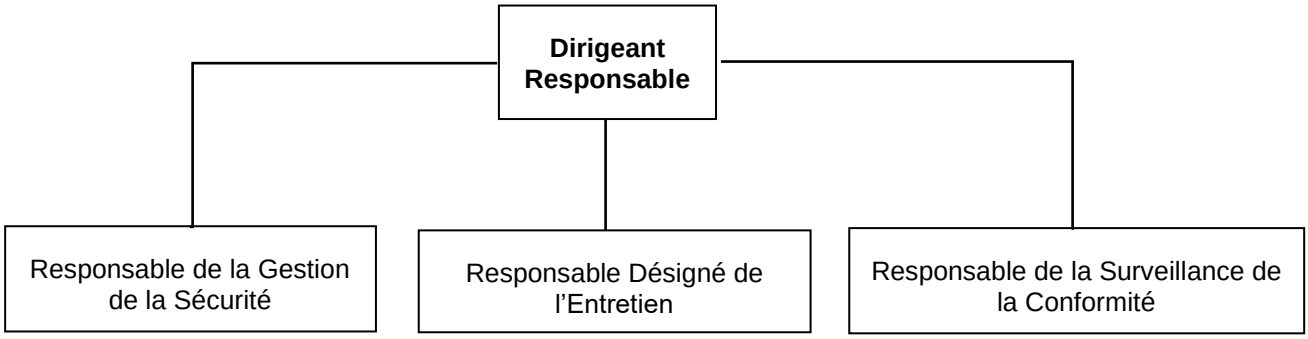
Elles sont reliées au Dirigeant Responsable qui porte la responsabilité ultime et directe (accountability) en matière de sécurité et de conformité, y compris financière. Ce dernier ne peut pas déléguer ses devoirs de comptabilité à la différence des autres personnes qui peuvent déléguer certaines de leur responsabilité.

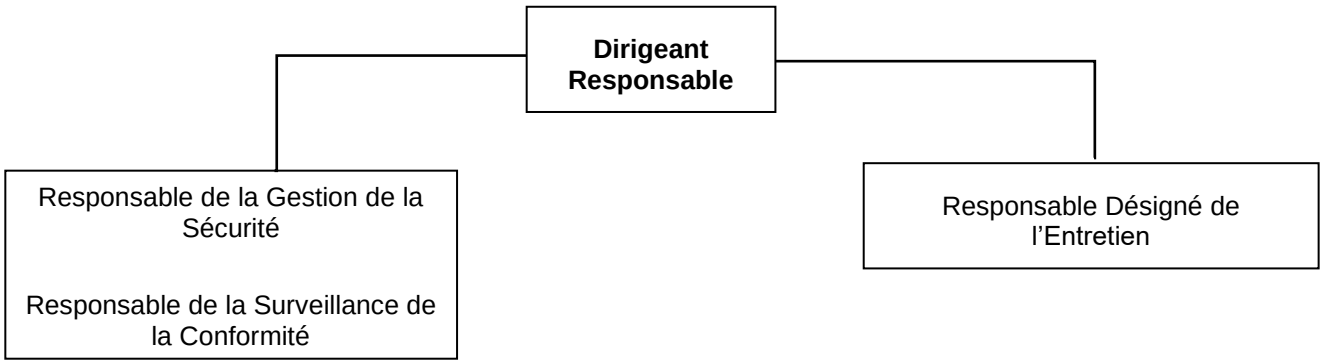
Cette chaîne de responsabilité au sein de l'organisme prévoit un système de retour d'information vers le DR pour permettre à ce dernier de s'assurer que les actions correctives et/ou événements de sécurité sont à la fois identifiés et rapidement pris en compte.

Ces fonctions sont réglementaires. L'intitulé exact des différentes fonctions (DR, RDE, RSC, RGS) est à la discrétion de l'exploitant, dans la mesure où il peut démontrer que celles-ci sont bien assurées.

Toutes modifications apportées aux personnels nommés ou aux rapports hiérarchiques entre les membres du personnel nécessitent une approbation préalable.

Exemples d'organigrammes :





3.2.2. Les postes clés

LE DIRIGEANT RESPONSABLE (DR)

Références réglementaires	
CAMO.A.200 (a)(1)	Système de gestion
CAMO.A.305(a)(b) *	Exigences en matière de personnel
AMC1 CAMO.A.305(a)*	Personnel requirements

Le Dirigeant Responsable (DR) :

- assure la responsabilité ultime et directe en ce qui concerne la sécurité, notamment en fixant les limites acceptables pour les risques de sécurité ;
- met à disposition les moyens financiers et humains nécessaires afin d'assurer les activités de gestion du maintien de la navigabilité ;
- est chargé d'établir et surveiller la performance et l'effectivité des actions en matière de sécurité et de conformité, par exemple en président le Safety Review Board (si applicable) ;
- définit la politique de sécurité et veille à son application ;
- définit les responsabilités des personnels en matière de sécurité/conformité ;
- veille à ce que les personnels responsables de la sécurité/conformité et des activités puissent le contacter directement pour le tenir dûment informé des questions de conformité et de sécurité.

D'autres exigences sont décrites dans l'AMC1 CAMO.A.305(a).

LE RESPONSABLE DÉSIGNÉ ENTRETIEN (RDE) – LA PERSONNE OU LE GROUPE DE PERSONNE

Références réglementaires	
CAMO.A.305(a)(3), (b)(2), (c)*	Exigences en matière de personnel
AMC1 CAMO.A.305(a)(3), (b)(2), (c)*	Personnel requirements

Il leur incombe la responsabilité de s'assurer que l'organisme respecte toujours les exigences applicables. Ils représentent la structure managériale de la gestion du maintien de la navigabilité et sont responsables à ce titre des opérations quotidiennes de l'organisme.

Critères communs :

- ils rendent compte en dernier ressort au dirigeant responsable ;
- ils ont les connaissances utiles, le cursus et une expérience satisfaisante dans le domaine de la gestion du maintien de la navigabilité et ils possèdent une connaissance réglementaire pratique ;
- ils ont également une connaissance des systèmes de gestion et des facteurs humains.

D'autres exigences sont notamment décrites dans l'AMC1 CAMO.A.305(c) notamment celles relatives aux connaissances et expériences techniques.

LE RESPONSABLE DE LA SURVEILLANCE DE LA CONFORMITE (RSC)

Références réglementaires	
CAMO.A.200(a)(6)	Système de gestion
CAMO.A.305(a)(4)*	Exigences en matière de personnel
AMC1 CAMO.A.305(a)(4)*	Personnel requirements

Généralités

Un responsable de la surveillance de la conformité (RSC) est désigné par le DR. Son rôle principal est de vérifier que les activités de maintien de la navigabilité sont conduites conformément aux exigences définies par l'organisme, elles-mêmes conformes à la réglementation. Il vérifie en outre que l'activité est effectivement supervisée par un responsable désigné (transporteurs aériens titulaires d'une licence) ou une structure managériale.

Il s'assure également :

- que toute maintenance contractée est gérée pour assurer la conformité à l'ordre de travail ;
- qu'un plan d'audit est correctement mis en œuvre, maintenu, amélioré et que des actions curatives et correctives sont demandées si nécessaire et correctement mises en œuvre.

Par ailleurs :

- il n'est pas un responsable du maintien de la navigabilité ;
- il a directement accès au DR ;
- il a accès à toutes les parties de l'organisation et si nécessaire, à celles des sous-traitants ;
- il justifie d'une compétence dans le domaine de la qualité/conformité ainsi que dans les domaines techniques. D'autres exigences sont décrites dans l'AMC1 CAMO.A.305(c) ;
- il justifie d'une connaissance de la réglementation applicable.

Le RSC peut s'appuyer sur un ou des correspondants conformité ayant des compétences spécifiques dans les différents domaines si lui-même n'a pas ces compétences. Il n'en garde pas moins toute sa responsabilité et reste le point focal en matière de conformité réglementaire.

Responsabilité de la surveillance de la conformité AIROPS et de la gestion du maintien de la navigabilité

Les règlements n'imposent pas d'avoir **une personne unique** identifiée comme étant en charge de la surveillance de la conformité des opérations AIROPS et du suivi de maintien de navigabilité CAMO. Ainsi un exploitant peut choisir d'avoir un responsable de la surveillance de la conformité pour les opérations dans le cadre de son CTA et un responsable de la surveillance de la conformité de la gestion du maintien de la navigabilité.

Ces deux responsables doivent toutefois respecter les exigences associées à ces fonctions, notamment :

- elles ont toutes deux un accès direct au dirigeant responsable ;
- l'organisation de l'exploitant permet la coordination et le pilotage nécessaire pour un retour d'expérience et des actions efficaces afin d'assurer l'intégration dans un système de gestion unique :
    - cohérence dans les procédures qualité/conformité ;
    - coordination dans l'élaboration du programme d'assurance qualité/conformité notamment pour des sujets transverses ;
    - coordination dans l'exploitation des résultats du programme d'assurance qualité/conformité.

Une indépendance hiérarchique entre ces deux personnes et un niveau équivalent de responsabilité favorisent l'équilibre entre les deux domaines à surveiller (opérations et maintien de la navigabilité).

Dans le cas d'un exploitant disposant d'un atelier Partie-145 intégré, l'exploitant peut également choisir d'avoir un responsable qualité pour la réalisation de l'entretien (Partie-145), en respectant les exigences d'un système qualité intégré.

Dans le cas contraire ou la surveillance de la conformité est sous la responsabilité d'une même personne, elle doit démontrer des compétences du domaine selon l'AMC1 CAMO.A.305(c).

LE RESPONSABLE DE LA GESTION DE SÉCURITÉ (RGS)

Références réglementaires	
AMC1 CAMO.A.200(a)(1)	Management system
AMC1 CAMO.A.305(a)(5)*	Personnel requirements

Le dirigeant responsable identifie un responsable qui gère l'élaboration, l'administration et le maintien de processus efficaces de gestion de la sécurité dans le cadre du système de gestion.
Il a un accès direct au DR mais reste le point focal en matière de sécurité et a accès à toutes les activités rentrant dans le périmètre du système de gestion.

Ses fonctions sont les suivantes :

- faciliter la gestion des risques ;
- surveiller la mise en œuvre des mesures prises pour atténuer les risques ;
- fournir des rapports périodiques sur les performances en matière de sécurité ;
- assurer la mise à jour de la documentation de gestion de la sécurité ;
- s'assurer que la formation à la sécurité est disponible et qu'elle répond aux normes acceptables ;
- donner des conseils sur les questions de sécurité ;
- assurer le lancement et le suivi des enquêtes sur les événements internes.

Le RGS doit pouvoir justifier de compétences en matière de gestion de la sécurité (formation, expérience, etc.).

LES RÈGLES DE CUMUL DE FONCTIONS

Certaines responsabilités peuvent être assumées par une même personne. Toutefois, l'encadrement doit être adapté à la taille et à la complexité de l'organisme, et chaque responsable doit pouvoir consacrer suffisamment de temps à sa fonction.

- **Cumul de la fonction de RDE avec d'autres fonctions**
  - **avec la fonction de DR**

Ce cas de figure est fréquent pour les petites structures. Un tel cumul n'est possible que si la charge de travail induite le permet. L'organisme s'assure alors que la personne est en mesure d'assumer l'ensemble des responsabilités liées à chacune des fonctions tenues (profil, compétences, temps alloué, etc.).

  - **avec d'autres fonctions de RD (AIR OPS)**

Un responsable désigné peut être responsable désigné dans d'autres domaines au sein d'un exploitant. Dans ce cas, le dirigeant responsable s'assure que la personne est en mesure d'assumer l'ensemble des responsabilités liées à chacune des fonctions tenues (profil, compétences, temps alloué, etc.).

- **Cumul de la fonction de RSC avec d'autres fonctions**

Le RSC ne peut pas être le RDE, la personne ou le groupe de personne (AMC1 CAMO.A.305(a)(4);(a)(5) §(b)(2)(c)) en raison du conflit d'intérêt inhérent.

Le RSC ne peut pas être le DR en raison du conflit d'intérêt inhérent sauf :

> *Sous réserve d'une **gestion des risques**, d'un **accord spécifique de l'autorité** compétente et **compte tenu de la taille de l'organisation et de la nature et de la complexité de ses activités**, le rôle de RSC ou RGS peut être exercé par le DR, pour autant qu'il ait démontré des compétences spécifiques.* **AMC1 CAMO.A.305 (a)(4);(a)(5) § (e) / §(b)(2)ii)**
>
> *Dans ce cas, le DR ne peut donc pas être l'un des RD en raison du risque de conflit d'intérêt entre RSC et RD.*
>
> *De plus, les audits devant être conduits par un personnel **indépendant**, ils ne peuvent pas être réalisés par le RSC lui-même.*

- **Cumul de la fonction de RGS avec d'autres fonctions**

Le RGS peut en théorie être le RDE. En pratique, l'organisme doit démontrer que les deux postes peuvent être effectivement être assumés par une même personne et qu'il n'y a pas de conflit d'intérêt notamment en termes de gestion de la sécurité.

Les fonctions de RGS et de RSC sont cumulables **AMC1 CAMO.A.305(a)(4); (a)(5) §(d)**. Cependant, le DR au regard de sa responsabilité directe et ultime en matière de sécurité, doit veiller à ce que des ressources suffisantes (temporelles et matérielles) soient allouées aux deux fonctions.

  - **avec le DR**

(Voir l'encadré supra).

EXTERNALISATION DES POSTES CLÉS

- **Cas d'un RSC externe**

La fonction de RSC peut être externalisée sous réserve que :

- la sous-traitance soit contractualisée ;
- la personne soit désignée nominativement dans le contrat de sous-traitance ;
- le temps alloué à cette personne, figurant dans le contrat, soit adapté à l'entreprise, l'exploitant vérifie notamment que les éventuels engagements extérieurs de cette personne sont compatibles avec les durées prévues dans le contrat ;
- la personne rapporte directement au DR de l'organisme ;
- la personne ait suivi une formation adéquate.

Le DR reste impliqué dans la fonction de surveillance de la conformité. Il surveille l'efficacité et l'effectivité des actions correctives de conformité (notamment à travers le haut comité de pilotage qu'est le Safety Review Board si applicable).

- **Cas d'un auditeur externe**

Références réglementaires	
AMC 3 CAMO.A.200(a)(6)	Contracting of the independent audit

Si du personnel externe est utilisé pour effectuer des audits indépendants :

- ces audits sont effectués sous la responsabilité du RSC ;
- l'organisme demeure responsable de s'assurer que le personnel externe possède les connaissances, les antécédents et l'expérience appropriés aux activités auditées, y compris les connaissances et l'expérience en matière de surveillance de la conformité ;
- l'organisme conserve la responsabilité ultime de l'efficacité de la fonction de surveillance de la conformité, en particulier de la mise en œuvre et du suivi efficaces de toutes les actions correctives.

- **Cas d'un RGS externe**

La fonction de RGS peut être externalisée sous réserve que :

- la sous-traitance soit contractualisée ;
- la personne soit désignée nominativement dans le contrat de sous-traitance ;
- le temps alloué à cette personne, figurant dans le contrat, soit adapté à l'entreprise ; l'exploitant vérifie notamment que les éventuels engagements extérieurs de cette personne sont compatibles avec les durées prévues dans le contrat ;
- la personne ait suivi une formation adéquate.

Toutefois, même en cas d'externalisation de la fonction de RGS, le DR conserve la responsabilité directe en ce qui concerne la sécurité.

3.2.3. Les instances de gouvernance

LE SAFETY REVIEW BOARD (SRB)

Références réglementaires	
AMC 1 CAMO.A.200(a)(1)	Management system

L'organisme met en place un SRB*. Ce comité de haut niveau réunit les principaux responsables en charge de la stratégie sécurité de l'organisme, en support du DR. Le SRB est présidé par le DR et réunit au minimum le RD ou la structure managériale, le RGS et le RSC.
Il s'agit d'une instance décisionnelle transversale.

Il a pour but de surveiller,

- **En matière de sécurité :**
  - les performances de sécurité par rapport à la politique et aux objectifs de sécurité ;
  - sue toute mesure de sécurité est prise en temps utile et que les décisions prennent en compte les éléments de sécurité ;
  - l'efficacité des processus du système de gestion de l'organisation ;
  - s'assurer que les ressources allouées sont suffisantes pour atteindre les objectifs de sécurité ;

- Il peut également surveiller en matière de conformité :
    - les résultats de la surveillance de la conformité ;
    - le suivi de la mise en œuvre des actions correctives et préventives associées ;

Lors de ces réunions, le SRB identifie et corrige les dérives pour empêcher, si possible, les non-conformités ou événements futurs. Les décisions prises lors de ces réunions sont tracées.
Le DR décide de la fréquence, de la forme et de la structure des SRB. Ces modalités sont à documenter. Une fréquence de deux réunions du SRB par an est adaptée. Cette fréquence est toutefois relative à la situation de l'exploitant (elle doit par exemple être avancée en cas de recrudescence d'événements de sécurité).

> ***AMC1 CAMO.A.200 (a)(1)(e) :** *Lorsque la taille de l'organisation, la nature et la complexité de ses activités le justifient, et sous réserve d'une évaluation des risques et d'un accord de l'autorité compétente, il peut ne pas être nécessaire que l'organisation crée un SRB. Dans ce cas, les tâches qui lui sont normalement attribuées doivent être attribuées au Responsable de la Gestion de la Sécurité.*

LE SAFETY ACTION GROUP (SAG)

Références réglementaires	
GM1 CAMO.A.200 (a)(1)	Management system

En fonction de la taille de l'organisation, de la nature et de la complexité de ses activités des **Safety Action Group (SAG)**, centrés sur des questions opérationnelles, peuvent être également être constitués de façon permanente ou temporaire.

A la différence du SRB qui est un comité de haut niveau, les SAG permettent de décliner et de coordonner la stratégie de sécurité à un niveau local, par exemple sur des questions de sécurité spécifiques portant sur la gestion du maintien de la navigabilité.

Ces membres sont porteurs de compétences spécifiques dont l'expertise est utile et sont issus de l'encadrement ou du terrain.

A titre d'exemple, ils peuvent :

- participer à la définition des axes de la stratégie de sécurité ;
- aider à la mise en œuvre de la stratégie de sécurité ;
- évaluer quelle incidence l'introduction de changements opérationnels ou de nouvelles technologies a sur la sécurité ;
- coordonner la mise en œuvre de toute action liée à des mesures de maîtrise des risques ;
- garantissent la mise en œuvre rapide de mesures spécifiques ;
- examinent l'efficacité de mesures spécifiques de maîtrise des risques.

3.3. Politique du système de gestion

Références réglementaires	
CAMO.A.200(a)(2)	Système de gestion
AMC1 CAMO.A.200(a)(2)	Management system

L'organisme doit décrire l'ensemble des philosophies et principes de l'organisme en matière de sécurité : c'est la politique de sécurité.

La politique de sécurité est un cadre faisant référence dans la gestion des activités en matière de sécurité. Elle en reflète les engagements, les objectifs généraux et fait la promotion d'une culture de sécurité positive. Elle annonce les « règles du jeu ».

Elle contient les principes de report interne et encourage le personnel à signaler les erreurs, incidents et dangers liés à la navigabilité ainsi qu'à coopérer à la surveillance de la conformité et aux enquêtes.

La politique de sécurité doit :

- être signée par le DR ;
- être diffusée et communiquée à l'ensemble des personnels de l'entreprise ;
- être périodiquement passée en revue pour rester pertinente et adaptée ;

C'est particulièrement le cas à l'occasion d'un changement du dirigeant responsable. Ce dernier doit revoir la politique de sécurité, afin d'évaluer le besoin de la modifier. A minima, le nouveau dirigeant responsable doit entériner formellement la politique existante.

Elle inclut un engagement à :

- se conformer à toutes les lois et exigences applicables et adopter les bonnes pratiques pour améliorer les normes de sécurité ;
- fournir les ressources nécessaires à la mise en œuvre de la politique de sécurité ;
- appliquer les principes des facteurs humains ;
- imposer la sécurité comme responsabilité majeure tous les responsables (elle doit être intégrée dans la gestion des activités) ;
- appliquer les principes de « culture juste » aux notifications d'événements et à leurs enquêtes et, en particulier, à ne pas mettre à disposition ni utiliser les informations sur les événements :

(i) pour attribuer le blâme ou la responsabilité au personnel notifiant pour des actions, omissions ou décisions prises par lui qui sont à la mesure de son expérience et de sa formation ; ou

(ii) à toute fin autre que le maintien ou l'amélioration de la sécurité aérienne.

La direction et les responsables doivent constamment promouvoir la politique de sécurité auprès de tout le personnel, démontrer leur engagement à son égard.

3.3.1. Les objectifs

Références réglementaires	
AMC1 CAMO.A.200(a)(2) (d)	Management system

L'organisme doit se fixer des objectifs relatifs à la prise en compte de la sécurité dans sa stratégie globale.
Ils correspondent **aux besoins de l'organisme lui permettant d'effectuer des activités sûres et conformes en régulant le déroulement de l'action**. Ils doivent être pertinents et évoluent donc dans le temps.

Ils reflètent les problématiques de sécurité et de conformité spécifiques à l'organisme, celles où des actions doivent être conduites.

Ils comportent :

- des buts précis à atteindre ;
- les actions nécessaires pour y parvenir ;
- les personnes impliquées dans leur réalisation et une affectation de temps et de moyens.

Les objectifs doivent être 'SMART' :

S : spécifiques
M : mesurables
A : atteignables
R : réalistes
T : temporels

Ils peuvent concerner ce qu'il faudrait atteindre (exemple : formations de personnels) ou ce qu'il faut éviter (exemple : non prise en compte de consignes de navigabilité).

Remarque importante :

Si leur finalité générale reste identique, **les objectifs doivent cependant avoir des granularités différentes pour améliorer l'efficacité des actions à conduire** : Les objectifs stratégiques ou généraux sont déclinés en objectifs intermédiaires et spécifiques.

Exemple :

Un organisme de gestion du maintien de la navigabilité se donne pour objectif « d'améliorer l'implication du Responsable Désigné dans la démarche d'amélioration de la sécurité ».

Il s'agit ici d'un objectif général qui, pour être mis en œuvre nécessite la définition d'objectifs intermédiaires à l'intention du RD : participer au traitement des événements de sécurité, établir une cartographie des risques, se former… et du DR : Financer les formations, étudier l'impact temporel par rapport à l'activité et apporter de nouveaux moyens le cas échéant, approuver la cartographie des risques, accompagner ce changement par des points réguliers….

Ces objectifs intermédiaires vont devenir pour les personnes en question des objectifs spécifiques encore plus fins à partir desquels ils mettront en œuvre actions adaptées :

- Participer au traitement des événements => Participer systématiquement aux enquêtes avec le responsable sécurité, mettre en œuvre les actions correctives identifiées, intégrer cette charge dans la gestion du temps…
- Etablir une cartographie => Appliquer le processus de gestion des risques à l'activité, intégrer les activités contractées, présenter les problématiques de sécurité en SRB… ;
- Formation => rechercher des formations utiles, les programmer…

Les objectifs doivent être accompagnés d'indicateurs et faire l'objet de revues régulières. Le Safety Review Board est un comité très adapté pour ces revues.

Par rapport aux attendus du système de gestion, les objectifs :

- constituent la base de la surveillance et de la mesure de la performance de sécurité ;
- reflètent l'engagement du maintien de l'efficacité du SG ;
- sont communiqués.

Le chapitre surveillance et mesure de la performance de la sécurité approfondira cette notion.

3.4. Gestion des risques

Références réglementaires	
CAMO.A.200(a)(3)	Système de gestion

3.4.1. Généralités

1/ Objectifs

Au regard de la multiplicité des organismes et des activités, une réglementation ne peut pas prescrire des règles de sécurité visant à encadrer l'ensemble des particularités. Le système de gestion permet d'aller au-delà de ces règles purement prescriptives, qui, si elles sont nécessaires pour la sécurité, nécessitent d'être complétées par des dispositions locales.
La gestion des risques vise à empêcher l'apparition d'événements ultimes lors d'une exposition à des dangers. Elle consiste à identifier les dangers, évaluer les risques inhérents afin de les hiérarchiser et, lorsque nécessaire, définir les actions d'atténuation ou de suppression qui permettent de maintenir les risques à un niveau acceptable.

2/ Définitions : *Dans le cadre de ce présent guide ces définitions sont applicables.*

Danger : Propriété intrinsèque des produits, équipements, procédés, situations… pouvant entrainer un dommage.

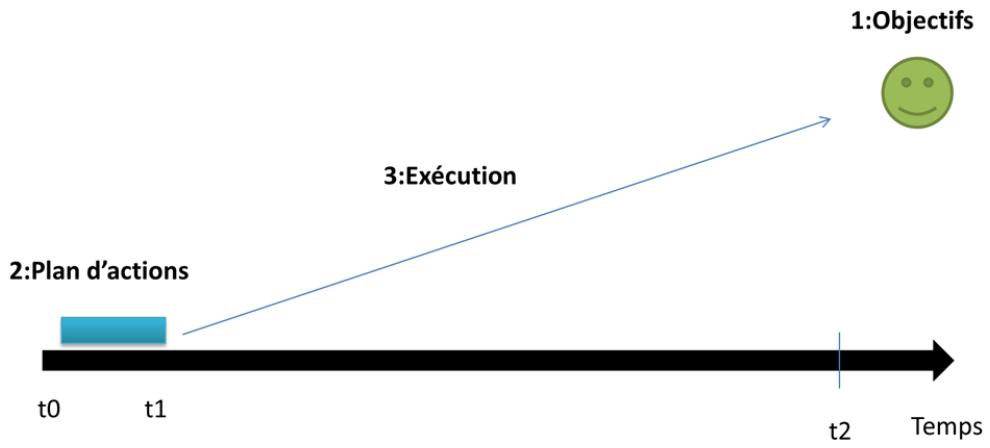
Risque : Le risque est la possibilité qu'un danger puisse exposer une cible (personne, aéronef, environnement) à un dommage. Il est caractérisé par le couple (gravité, probabilité).

Sécurité : État dans lequel les risques liés aux activités aéronautiques concernant, ou appuyant directement, l'exploitation des aéronefs sont réduits et maîtrisés à un niveau acceptable.

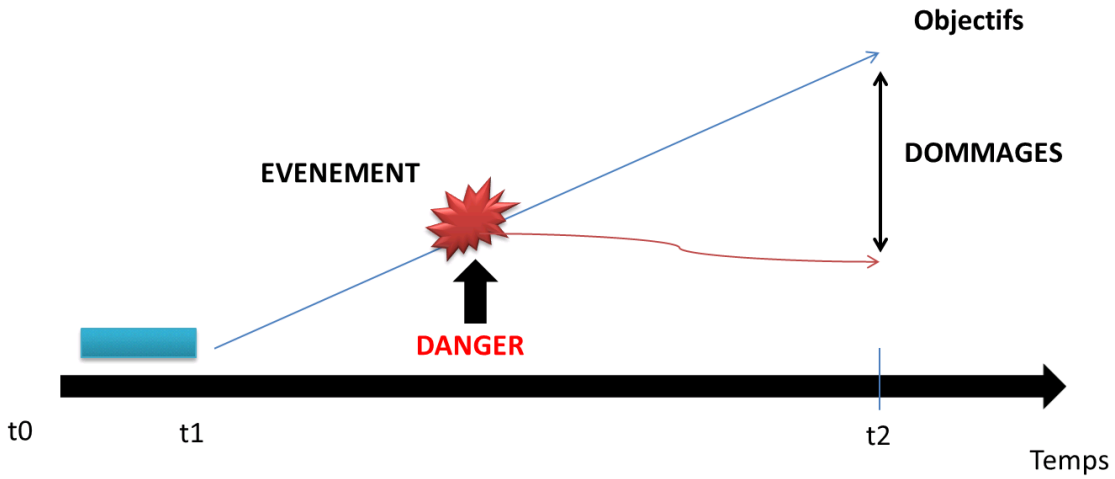
Dommage (événement ultime) : Evénement regrettable (pour la santé, l'environnement, le matériel…). Peut être considéré comme un point de non-retour.

Événement redouté (ou indésirable…de nombreux termes sont utilisés) : C'est une entrave à l'atteinte des objectifs. Elle est liée aux dangers. Ce type d'événement peut être considéré comme une perte de maîtrise du processus opérationnel.

Application : Pour atteindre ses objectifs, un organisme met en place des mesures à travers un plan d'actions (entre les dates t0 et t1).

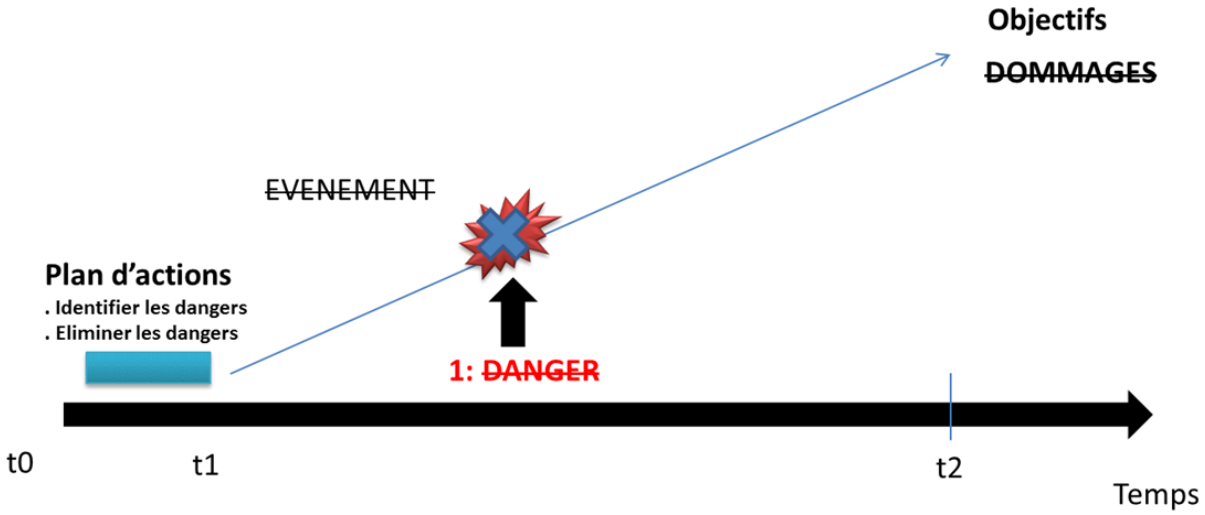


Des événements, liés à la rencontre de dangers peuvent perturber l'exécution du plan d'action et empêcher l'atteinte des objectifs. Les conséquences de l'accident au regard des objectifs sont appelées **dommages**.



3/ Quelles possibilités pour gérer le risque ?

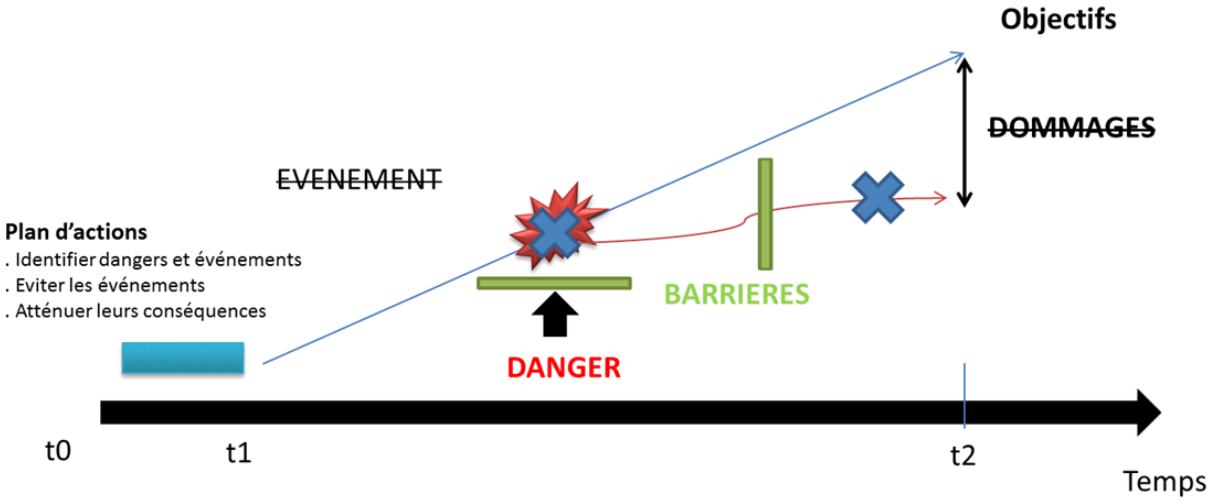
Une première option consiste à **éliminer** les dangers. Ainsi, plus de danger, plus d'événement (et plus d'événement, plus de dommages).



=> Dans ce cas la sécurité peut être définie comme l'absence de danger.

Exemple : Une organisation n'investit pas dans un nouveau logiciel de gestion du maintien de la navigabilité qu'elle estime trop complexe à maîtriser.

Une autre option consiste à **éviter les événements et réduire leurs conséquences à un niveau acceptable** ou supprimer le couple événements-dommages. Pour cela, **des barrières** cassant la relation entre danger, événement et conséquences sont mises en place. Un danger ne conduit alors plus à un événement (et plus d'événement, plus de dommages).



Ces barrières peuvent être multipliées : on introduit ici la notion de **défense en profondeur**.

Une phase préparatoire va permettre de prévoir et de mettre en place les barrières de défense.
Une fois les barrières de défense en place, il est nécessaire d'évaluer la possibilité de défaillance de ces barrières, puis le risque résiduel. Il restera à statuer sur l'acceptabilité de ce risque.

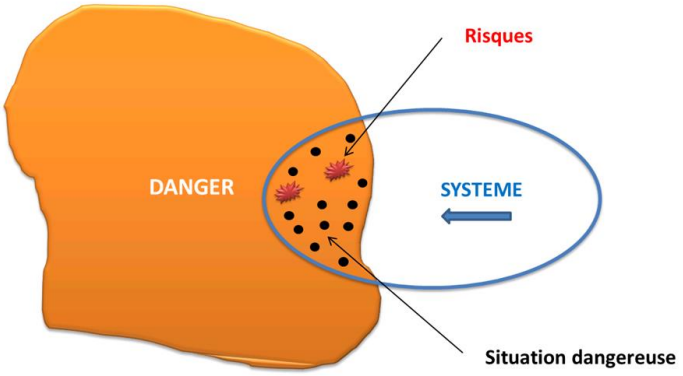
=> Dans ce cas la sécurité est définie comme l'absence de risques inacceptables.
(Principe de réduction du risque)

Exemple : Si l'organisation investit finalement dans un logiciel de gestion du maintien de la navigabilité jugé complexe, elle devra déterminer les événements redoutés possibles ainsi que leurs conséquences et mettre en place un système de défense pour éviter leur survenue (formation, entrainement, assistance…).

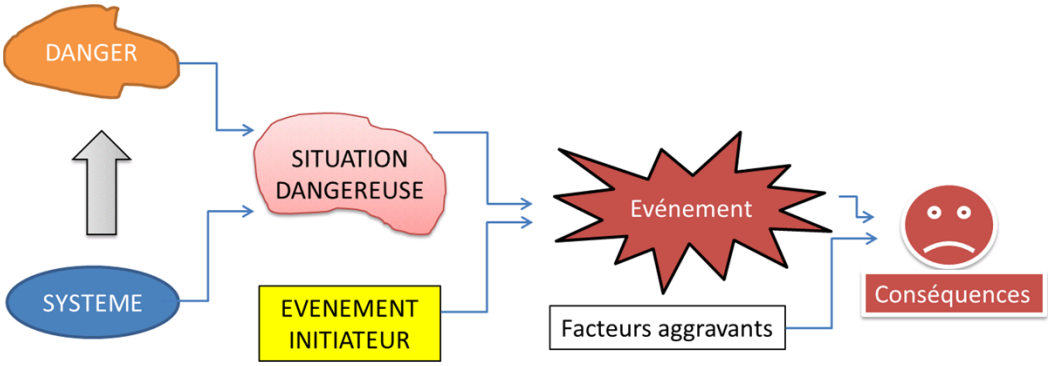
Note : La gestion de la sécurité est effectuée pendant la phase d'étude mais également pendant la phase d'exécution notamment par **le retour d'expérience** : *nouveaux dangers, nouveaux accidents possibles, connaissance de l'efficacité et de la fiabilité de barrières.*

4/ Une modélisation du processus du risque

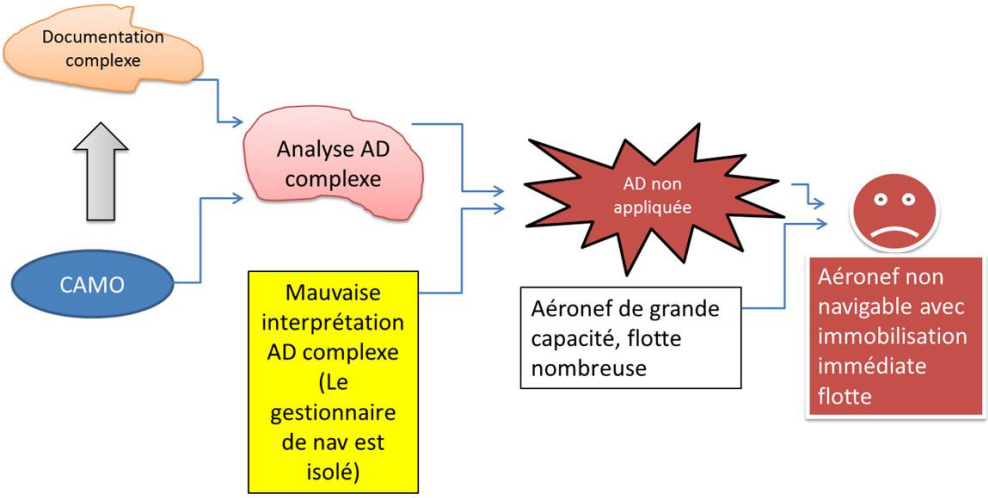
Cette modélisation reprend des éléments observables : Un système (par exemple l'organisation) rencontre un danger. Il se retrouve alors dans une situation dangereuse avec des risques de survenue d'événements et leurs conséquences associées.



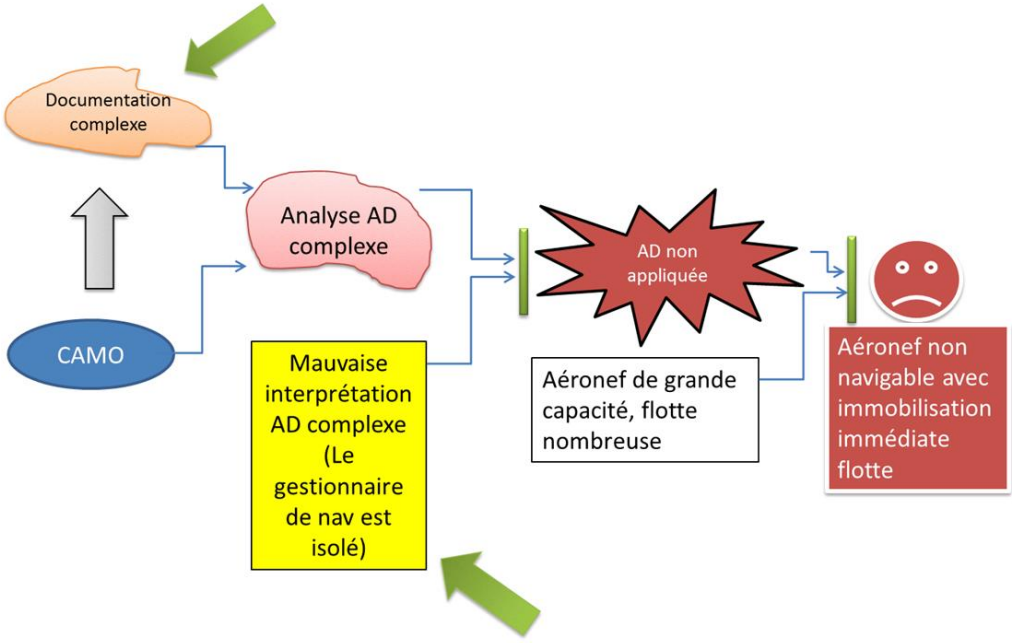
Cette représentation peut se décliner en scénario d'accident avec l'introduction de facteurs initiateurs et aggravants.



Exemple appliqué à la gestion du maintien de la navigabilité :



A partir de ces scénarios on peut éliminer les dangers, prévenir les événements initiateurs, éviter les événements redoutés et limiter les conséquences en cassant les relations dans l'enchainement.



Les mesures prises sont souvent dénommées « barrières ». On en distingue généralement deux catégories principales, dont les noms peuvent varier :

Les barrières de prévention : Ensemble des moyens ou mesures qui permettent de réduire les risques auxquels on peut être exposé.

Les barrières de protection : Ensemble des moyens ou mesures qui permettent de limiter les conséquences d'un événement.

Note : Il est parfois question de barrières de **Récupération à la place de « Protection »**. Elles renforcent *la prévention en récupérant une situation de perte de maîtrise.*

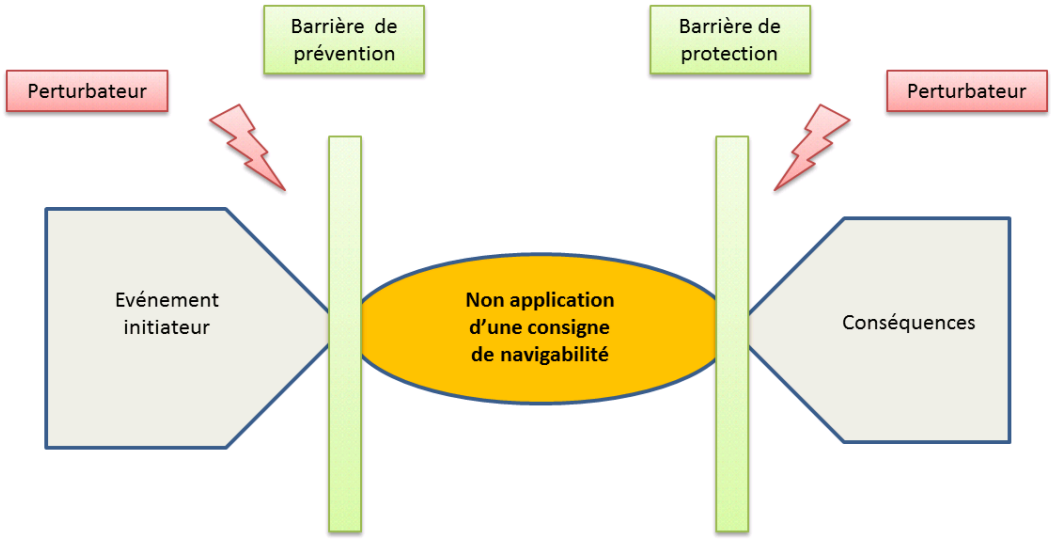
Des perturbateurs peuvent venir diminuer l'efficacité des barrières.

Exemple appliqué au cas ci-dessus :

Barrières de prévention : Demande de clarification systématique au constructeur en cas de doute, Relecture commune des AD jugées complexes avec une entité compétente interne (autre personnel CAMO, Qualité, 145) ou externe (CAMO d'une autre organisation) ….

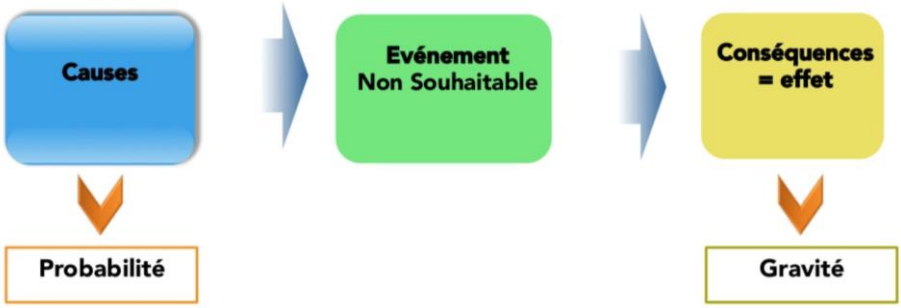
Barrières de protection : Revue de prise en compte des AD…. Il s'agit ici de détecter au plus tôt une AD non appliquée.

Perturbateurs des barrières : tensions internes freinant la communication interservices, pression productive, manque de rigueur….



5/ Mesurer le processus du risque
(Des exemples sont présentés au § analyse des risques)

On évalue le risque en tenant compte de la probabilité et de la gravité.



En ce qui concerne la possibilité de survenue de l'événement :
On cote la probabilité de survenue à partir de l'identification de l'événement initiateur. On peut y rajouter la fréquence d'exposition (ou la durée) à la situation dangereuse.

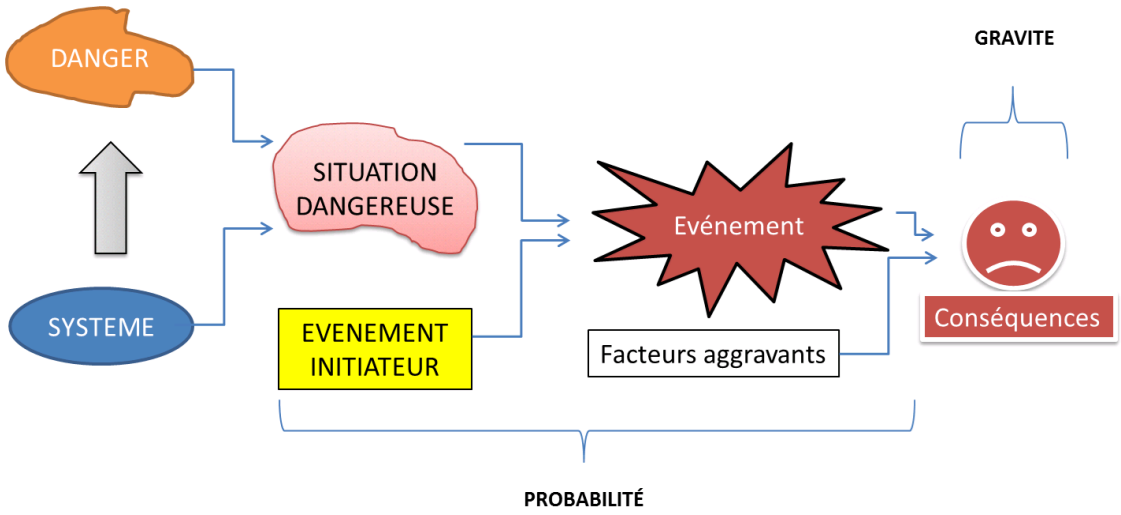
Il existe une relation entre l'événement initiateur et l'événement redouté (non souhaitable) avant la mise en place de barrières : l'un entraine l'autre. L'évaluation de la survenue de l'un est donc égale à l'évaluation de la survenue de l'autre.

Exemple : Une erreur d'interprétation d'une AD complexe entrainera un défaut dans son application.

En ce qui concerne la gravité des conséquences :
On estime l'importance des dommages (blessures, mort, pertes matérielles, financières, retard en exploitation…).

Remarques :

- il est impossible de cerner et d'évaluer tous les scénarios de risque ;
- il est particulièrement difficile non pas de définir des effets potentiels liés à un événement redouté mais de définir la probabilité de survenue de chacun. Les possibilités deviennent très nombreuses.



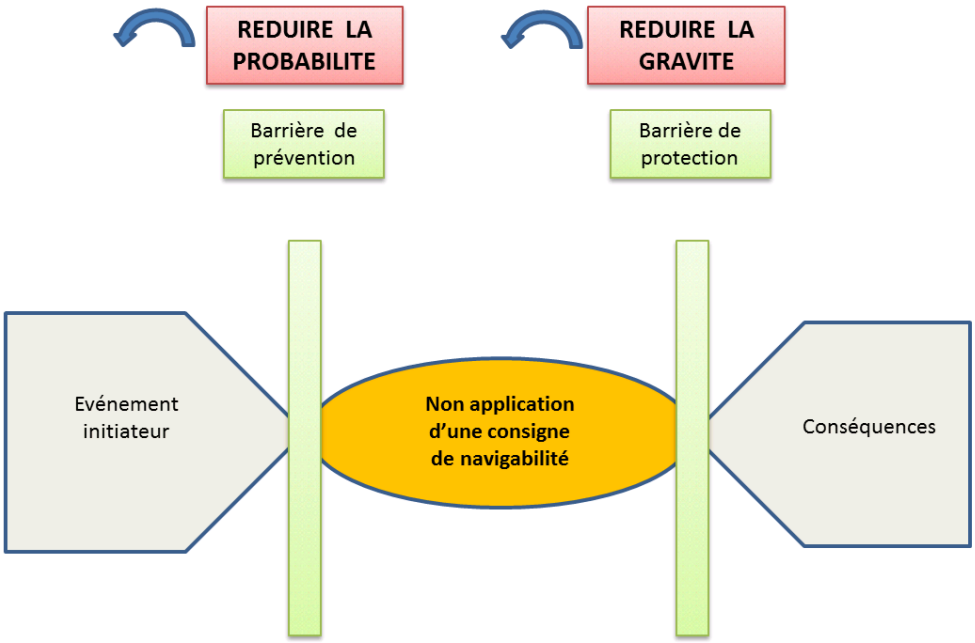
Mesurer le processus avec les barrières :

Les barrières de prévention permettent de réduire la probabilité de survenue d'un événement redouté.
C'est la probabilité de l'événement redouté après l'instauration des barrières de prévention que l'on va prendre en compte pour évaluer le risque.

Les barrières de protection permettent de réduire la gravité des conséquences (si le dommage survient il est moindre).
Note : Certains modèles, prennent en compte ces barrières pour déterminer la probabilité finale de survenue des conséquences.

Attention ! La mesure du processus prend en compte des barrières supposées être adaptées, effectives et efficace.

<u>Un enjeu majeur en matière de sécurité est la gestion de ces barrières sur le terrain.</u>



Conclusion sur la modélisation du risque :

Il n'y a pas de modèle universel du risque. Chaque organisme adopte le modèle de risque adapté à son activité.

La modélisation n'est qu'une simplification de la réalité, beaucoup plus complexe.
Attention à ne pas en faire une certitude et à ne pas s'enfermer dans une logique strictement technique car les causes d'un accident sont multi critères, contextuelles et aléatoires.

La gestion de la sécurité est aussi la gestion de l'aléa et de l'incertitude !

Il faut développer un échantillonnage cohérent de risques qui générera une gamme de mesures d'atténuation.

3.4.2. Le processus de gestion des risques

Références réglementaires	
AMC1 CAMO.A.200(a)(3) (a)(b)	Safety management key process

Ce processus doit permettre d'assurer :

- l'identification des dangers pour la sécurité aérienne qui découlent des activités,
- l'évaluation et la gestion des risques associés à ces dangers,
- la prise de mesures destinées à atténuer les risques,
- la vérification de l'efficacité de ces mesures d'atténuation.

3.4.2.1. L'identification des dangers

Les dangers sont porteurs d'un potentiel de nuisance pour l'être humain ou ses activités. Ils sont des éléments de nature très variées (énergies, toxicité, propriétés dangereuses, situations dangereuses, défaillances, interactions…).

Leur connaissance est utile car ils renseignent sur :

- ce qui peut conduire à un événement ;
- la nature des dommages possibles (ils dépendent directement de la nature du danger) ;
- la définition de moyens d'évitement des événements.

Exemple en matière de gestion du maintien de la navigabilité :

-Danger : Logiciel de gestion de maintien de la navigabilité complexe
-Nature des dommages : Aéronef non navigable
-Moyens d'évitement : barrières autour de la formation et de l'accompagnement des personnels

L'identification des dangers se fait à différents niveaux :

- les moyens **réactifs** analysent des résultats ou des événements du passé (*exemple : la remontée d'événements ou de problématiques de conformité*) ;
- les moyens **proactifs** déterminent si un danger pourrait entraîner un accident ou un incident en recherchant activement les conditions dangereuses dans les processus existants de l'organisme *(exemple : les études de sécurité portant sur une activité ou les études de changement*).

Cette identification doit comprendre :

- les dangers pouvant découler des limitations **des performances humaines**.
  Note : Nous avons vu qu'il est également important de prendre en compte **les facteurs organisationnels.**
- les dangers pouvant résulter de l'existence de **dispositions complexes en matière d'exploitation et de maintenance** (*par exemple, lorsque plusieurs organisations sont sous-traitées ou lorsque plusieurs niveaux de contrat / sous-traitance sont inclus*).

Remarque : Les dangers relatifs à la gestion du maintien de la navigabilité ne sont pas évidents à identifier comme peuvent l'être des énergies *(danger de l'électricité par exemple).*

L'expérience montre par exemple que ce qui est porteur d'un potentiel de nuisance pour ces activités est du domaine de l'humain (propriétés, comportement…), de l'organisationnel (dysfonctionnements impactant la réalisation des tâches ou des comportements, coopération entre diverse entités…), des logiciels de gestion de navigabilité, de la complexité de la documentation ou d'erreurs documentaires…

Ces dangers moins évidents ne produisent pas moins d'effets et peuvent être à l'origine de dommages importants *(panne d'un système entrainant la destruction de l'aéronef par exemple).*

Si l'identification des dangers permet de connaitre les menaces possibles et leurs conséquences, il faut ensuite s'intéresser à leurs effets (les événements).

Or s'intéresser à l'événement c'est déterminer **le risque** de survenue de l'enchainement :

Danger (cause) **=> Evénement** (effet) **=>Dommage** (conséquences)

L'identification des dangers puis des risques associés permet donc de répondre à la question :
*Quels sont les **risques possibles d'événements** entravant nos objectifs de maintien de la navigabilité des aéronefs et de préservation des personnes ?*

Exemple :

L'organisme analyse son activité et cherche les risques inhérents à son exploitation.

-Quels sont mes dysfonctionnements ?
- Que m'est-il arrivé ?
- Qu'est-il arrivé aux autres ?
- Que pourrait-il m'arriver d'autre ?

Note : Grâce à l'identification des risques, on peut remonter aux dangers. Ce point de départ est parfois préféré.

1/ Principes communs à l'identification des dangers et des risques

Il convient de respecter deux principes clés :

- l'identification doit laisser libre cours à l'investigation ou à la projection ;
- **chacun n'a qu'une part des informations et des savoirs nécessaires à la sécurité ! L'identification doit être menée avec les spécialistes métier.**

2/ Exemples d'outils d'identification des dangers et des risques associés (non exhaustif)

➢ **La veille (moyens réactifs et proactifs)**

L'organisme appuie sa veille sur des sources d'information variées :

- événements internes : recueil d'événements (règlement (UE) n°376/2014) et leur traitement ;
- résultats de la surveillance ;
- analyse et étude de changement passés… ;
- veille externe (BEA, info sécurité DGAC, SIB EASA…) ;
- …

➢ **Le brainstorming (moyen réactif / proactif)**

L'idée générale de la méthode est la récolte d'idées nombreuses et originales.
Deux principes de base définissent le brainstorming :

- la recherche la plus étendue possible ;
- la suspension du jugement.

➢ **Le diagramme d'Ishikawa (moyen réactif)**

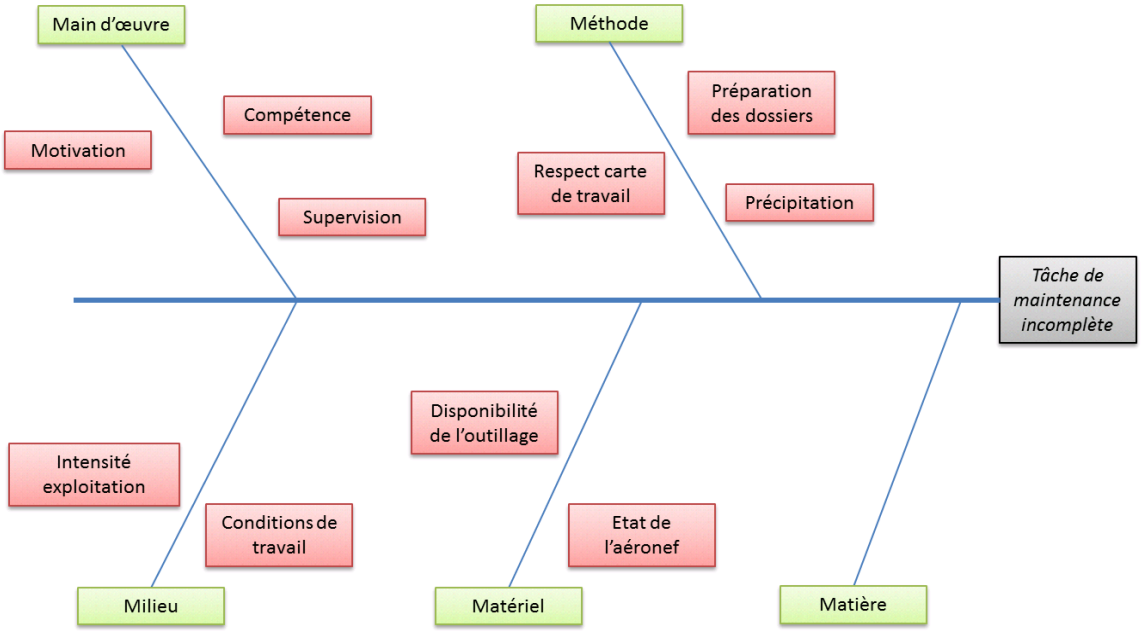
Après la survenue d'un événement, un groupe de travail effectue un brainstorming afin de rechercher toutes les causes possibles à l'aide de cet outil.

Les causes sont regroupées par famille (5M) :

Les causes Potentielles	**Les familles**
Personnel, qualifications, formation, expérience, etc.	**Main d'œuvre**
Equipement, machine, vitesse, paramètres fonctionnels, outils etc.	**Matériel**
Matière première, composant, matériau, pièce, etc.	**Matière**
Spécifications, plan, instructions procédures, etc.	**Méthode**
Espace, lumière, bruit, météo, environnement	**Milieu**

Le diagramme représente de façon graphique les causes aboutissant à un effet.

Exemple :



- **Les 5 Pourquoi (moyen réactif)**

Il s'agit de poser la question pertinente commençant par un pourquoi afin de trouver la source, la cause principale de l'événement.

Exemple :
1. Pourquoi y-a-t-il eu un dépassement de consigne de navigabilité ? - Non prise en compte d'alertes de butée destinées à un autre service
2. Pourquoi (non prise en compte d'alertes…) ? – Manque de communication
3. Pourquoi (...) ? – Cloisonnement des collectifs
4. Pourquoi (…) ? – Manque d'objectifs partagés
5. Pourquoi (…) ? – Manque de définition d'objectifs internes par la direction

- **Le nœud papillon (bowtie – moyen proactif)**

Le nœud-papillon focalise la représentation du risque autour d'un événement central représentant l'événement (redouté central, indésirable, accidentel…).
Sur cette représentation graphique, les **causes** de cet événement apparaissent à gauche de l'événement. Les **conséquences** de l'événement apparaissent à droite.

Exemple :

Le CAMO d'un organisme est composé d'un RDE et d'un agent de navigabilité.
- Le poste de responsable désigné connait des rotations de personnel régulières laissant l'agent de navigabilité seul.
- Le logiciel de gestion du maintien de la navigabilité connait des dysfonctionnements.

En considérant par exemple la publication de consignes de navigabilité urgentes (modification avant le prochain vol) dont est redevable la flotte, on peut s'interroger sur les dangers et les risques associés.

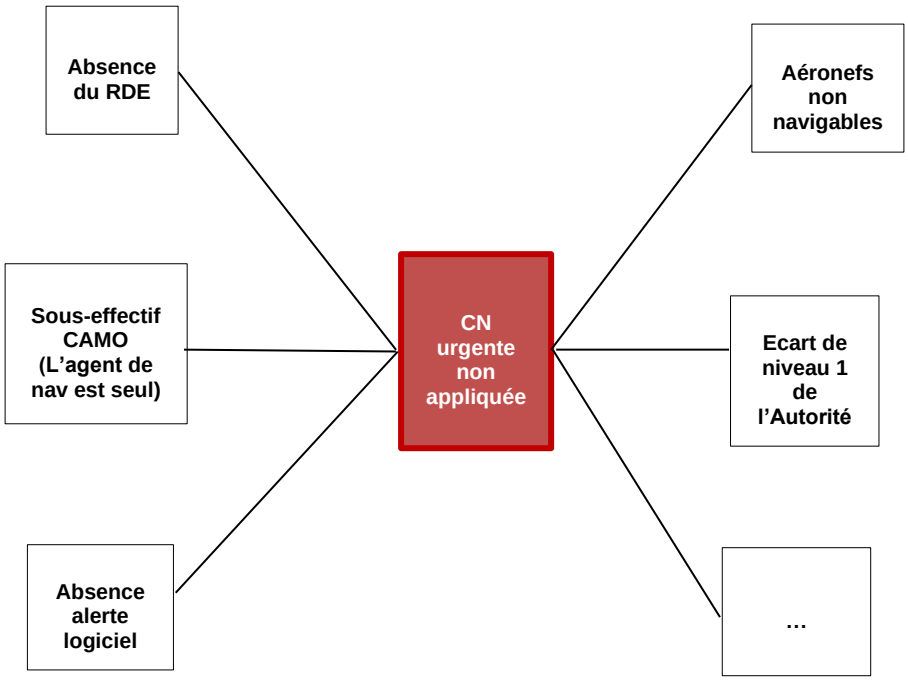
Dangers : Dysfonctionnements organisationnels et techniques (logiciel).

Situation dangereuse : Réaliser des tâches de gestion du maintien de la navigabilité dans un environnement dysfonctionnel. La gestion du maintien de la navigabilité se heurte aux dysfonctionnements. Elle est en sous-effectif pour effectuer l'ensemble de ses tâches et le logiciel ne fonctionne pas de façon optimale.

Risque : Non application d'une CN urgente.

Evénement initiateur : Non prise en compte d'une CN urgente.

Détermination de causes et de conséquences :



Note : L'identification a pour objectif d'identifier les risques possibles. Il ne s'agit pas d'avoir une connaissance profonde de chacun d'eux. La représentation des causes et de conséquences ne devra pas aller trop loin à ce stade du processus.

3.4.2.2. L'analyse des risques

Elle va permettre de mieux connaitre la nature des risques identifiés. Elle va tout d'abord s'interroger sur leur réalité puis estimera ensuite leur degré d'importance.

Etape 1

- Se questionner sur la **réalité des risques** recensés dans l'étape précédente. Lesquels concernent réellement mon activité ou une situation donnée ?

L'intérêt de cette étape est de sélectionner les risques dont on estime qu'ils nécessitent une analyse plus approfondie. Cette démarche allège les cartographies des risques des organismes.

Etape 2

- Se questionner sur **le degré d'importance des risques effectifs**.

Deux attributs sont considérés pour estimer le degré d'importance du risque :

- La **probabilité que l'événement survienne** ;
- La **gravité des dommages (conséquences).**

*Exemple de grille de détermination de la **probabilité** (Source OACI) :*

Probabilité	*Signification*	*Valeur*
Fréquent	Susceptible de se produire de nombreuses fois (s'est produit fréquemment)	**5**
Occasionnel	Susceptible de se produire parfois (ne s'est pas produit fréquemment)	**4**
Faible	Peu susceptible de se produire, mais possible (s'est produit rarement)	**3**
Improbable	Très peu susceptible de se produire (on n'a pas connaissance que cela se soit produit)	**2**
Extrêmement improbable	Il est presque inconcevable que l'événement se produise	**1**

*Exemple de grille de détermination de la **gravité** (Source OACI) :*

Gravité	*Signification*	*Valeur*
Catastrophique	Aéronef/équipement détruit Multiples décès	**A**
Dangereux	Importante réduction des marges de sécurité, détresse physique ou charge de travail telle qu'il n'est pas sûr que les opérateurs pourront accomplir leurs tâches de façon exacte ou complète Blessures graves Importants dommages aux équipements	**B**
Majeur	Importante réduction des marges de sécurité, réduction de la capacité des opérateurs à faire face à des conditions de travail défavorables, du fait d'une augmentation de la charge de travail ou en raison de conditions compromettant leur efficacité Incident grave Personnes blessées	**C**
Mineur	Nuisance Limites de fonctionnement Recours à des procédures d'urgence Incident mineur	**D**
Négligeable	Peu de conséquences	**E**

Exemple :

Un des risques identifiés lors de la recherche est le suivant : ***Réalisation d'une tâche d'entretien par un organisme non approuvé pour la tâche d'entretien en question****.*

Cas 1. L'organisme n'a pas contracté un autre organisme. Il n'est donc pas concerné par ce risque pourtant bien réel dans la gestion du maintien de la navigabilité.

*Cas 2. L'organisme a contracté un autre organisme. Il est concerné par ce risque. La connaissance de l'organisme contracté, les garanties apportées et la robustesse du système de gestion du CAMO montrent que la probabilité du risque est « **Improbable** ».*
*En revanche, l'analyse montre que des cas se sont produits dans d'autres organismes par défaut de contrôle et ont eu pour conséquences des aéronefs non navigables voir des dégâts matériels. La gravité est estimée « **Dangereux** ».*

Le degré d'importance du risque est donc établi comme suit dans le cas n°2 : La vraisemblance de ce risque est improbable et ses conséquences pourraient être dangereuses.

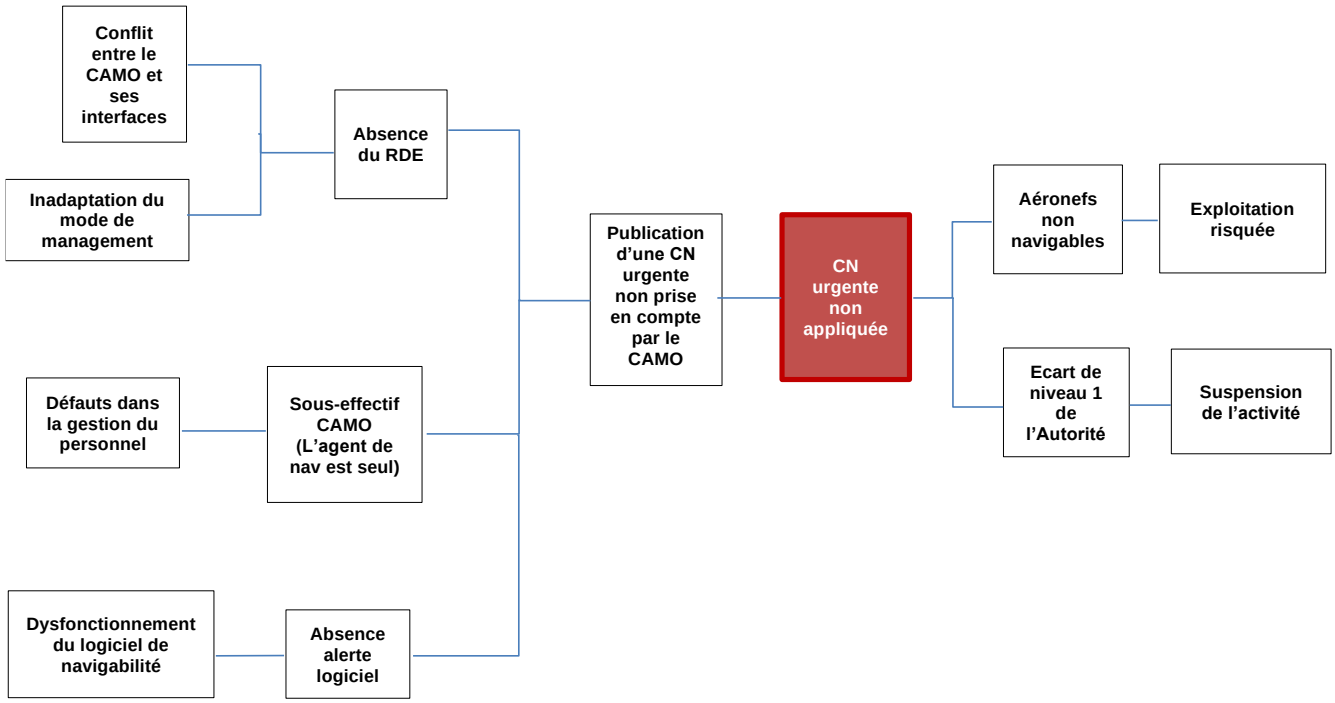
Exemple d'outil utilisé lors de cette phase : Le nœud papillon

Détailler les causes
Le nœud-papillon est tout d'abord utilisé lors de l'analyse du risque en étendant les branches gauches pour décrire des sous-causes des causes voire des **causes profondes**.
L'approfondissement des causes nous permet ainsi de nous questionner sur la réalité du risque étudié : ce scénario est-il crédible ?

Détailler les conséquences
Le nœud-papillon peut également être étendu dans sa partie droite dans un but d'étude des conséquences secondaires issues de conséquences primaires.

Note : Les barrières déjà existantes devraient être prises en compte.

Exemple :



Le nœud papillon permet d'alimenter une matrice du processus du risque (exemple de scénario) :

SITUATION DANGEREUSE	EVENEMENT INITIATEUR	*EVENEMENT REDOUTE*	CONSEQUENCES	PROBABILITE	GRAVITE
Réalisation de tâches de gestion du maintien de la navigabilité dans un environnement dysfonctionnel	Publication d'une CN urgente non prise en compte par le CAMO	***Non application d'une CN urgente***	Aéronef non navigable	**Occasionnel (4)**	**Catastrophique (A)**

3.4.2.3. L'évaluation des risques

L'évaluation mesure le risque **en combinant** les valeurs des deux attributs fournis par l'analyse : La **probabilité d'occurrence de l'événement** et la **gravité des dommages**.
Cette combinaison nous fournit un **niveau du risque qui sera comparé aux critères d'acceptabilité.**

Etape 1 : Etablir le niveau de risque

Un outil très classique pour mettre en œuvre cette combinaison est la **matrice de risque.**

Exemple lié au cas évoqué supra : la combinaison « improbable » et « dangereux » nous donne une évaluation du risque « Bas ».

	Catastrophique	**Dangereux**	**Majeur**	**Mineur**
Fréquent	Haut	Haut	Intermédiaire	Bas
Occasionnel	Haut	Intermédiaire	Intermédiaire	Bas
Faible	Intermédiaire	Intermédiaire	Bas	Bas
Improbable	Bas	Bas	Bas	Bas

Autre exemple avec la matrice issue du manuel SMS de l'OACI. Elle est utilisée de la façon suivante : si pour une situation étudiée, la vraisemblance a été estimée à « Faible », par exemple, et la gravité à « Dangereux » lors de l'analyse, cette matrice évalue le niveau de risque à « 3B ».

Tableau 3. Exemple de matrice d'évaluation des risques de sécurité

Risque de sécurité		*Gravité*				
Probabilité		*Catastrophique A*	*Dangereux B*	*Majeur C*	*Mineur D*	*Négligeable E*
Fréquent	5	5A	5B	5C	5D	5E
Occasionnel	4	4A	4B	4C	4D	4E
Faible	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extrêmement improbable	1	1A	1B	1C	1D	1E

Etape 2 : Définir l'acceptabilité du risque

Dans une seconde étape, le niveau de risque doit être qualifié de risque acceptable ou non. Généralement, **le niveau de risque acceptable** est stipulé. Les niveaux inférieurs ou égaux à ce seuil sont considérés comme acceptables et les niveaux supérieurs sont qualifiés d'inacceptables.

Le niveau orange nécessite ici un suivi.

Plage de l'indice de risque de sécurité	*Description du risque de sécurité*	*Mesure recommandée*
5A, 5B, 5C, 4A, 4B, 3A	INTOLÉRABLE	Adopter des mesures immédiates pour atténuer le risque ou arrêter l'activité. Réaliser une atténuation prioritaire des risques de sécurité afin de garantir que des contrôles préventifs additionnels ou renforcés sont en place pour abaisser l'indice des risques de sécurité à un niveau tolérable.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	TOLÉRABLE	Peut être toléré en fonction de l'atténuation des risques de sécurité. Cela peut nécessiter une décision de la direction en ce qui concerne l'acceptation du risque.
3E, 2D, 2E, 1B, 1C, 1D, 1E	ACCEPTABLE	Acceptable en l'état. Aucune autre mesure d'atténuation du risque n'est nécessaire.

Exemple de la matrice du processus du risque complétée :

SITUATION DANGEREUSE	EVENEMENT INITIATEUR	EVENEMENT REDOUTE	CONSEQUENCES	PROBABILITE	GRAVITE	EVALUATION AVEC ACCEPTATION
Réalisation de tâches de gestion du maintien de la navigabilité dans un environnement dysfonctionnel	Publication d'une CN urgente non prise en compte par le CAMO	***Non application d'une CN urgente***	Aéronef non navigable	**Occasionnel (4)**	**Catastrophique (A)**	**4A INTOLERABLE**

Attention ! La définition de l'acceptabilité de la matrice de risque est issue de choix de l'organisme et du DR, souvent sociétaux (acceptabilité sociale des événements graves). La définition des seuils est de la responsabilité du dirigeant responsable. Elle doit être cohérente avec **l'exigence de sécurité de l'activité**.

Il faut également prendre en compte la subjectivité de l'évaluation des risques en fonction de différents critères :

- **la relativité des résultats de l'analyse** : Les résultats peuvent différer au sein du groupe d'évaluation, quel avis retenir ?
- **le coût du traitement :** S'il est très élevé, il va augmenter la tolérance au risque ;
- **le bénéfice du risque** : L'acceptation du risque peut comporter des avantages (pour l'exploitation par exemple) ;
- **les attitudes face au risque** : Les individus ayant de l'aversion au risque vont les surévaluer. Ceux qui ont l'appétit du risque (ou goût du risque) vont les sous-évaluer.

Remarques :

La sécurité des vols est la résultante de la globalité d'un système : conception, maintien de la navigabilité, exploitation, gestion du trafic….
Des organismes ne sont pas reliés directement aux opérations aériennes (organismes d'entretien, organismes de gestion du maintien de la navigabilité non associés à un CTA, etc.). Ils contribuent pour autant positivement ou négativement à la sécurité des vols.

La question se pose sur la détermination des conséquences des événements redoutés dans le cas des études proactives :

- Faut-il les intégrer aux opérations aériennes ?
Cette démarche rend les conséquences plus concrètes mais complexifie la détermination de la probabilité des scénarios et de leur gravité. Cette évaluation relève des compétences du concepteur de l'aéronef.

-Faut-il les laisser au niveau « métier » ?
Les scénarios sont plus réalistes et se focalisent sur la sécurisation des activités de maintien de la navigabilité, ce qui est exigé. Il est cependant plus difficile d'évaluer la gravité pour prioriser les risques
En effet, si l'on considère l'événement ultime de ce type d'activité comme étant un *aéronef non navigable,* il est difficile d'en évaluer la gravité : un aéronef est navigable ou il ne l'est pas.

On constate alors que la sécurité dans les activités de maintien de la navigabilité **est principalement assurée par les mesures de prévention.** Ainsi, faire une cartographie des risques pertinente dans ce domaine, c'est se poser la question suivante : **qu'est-ce qui dans mon organisation va venir perturber la bonne exécution des tâches de maintien de la navigabilité ?**

On peut par exemple se référer aux six thèmes suivants développés au §2 de l'annexe en fin de guide pour identifier des dangers :
- les conditions de travail ;
- l'organisation du travail ;
- la communication-coordination-concertation ;
- la gestion du temps ;
- la formation ;
- la définition et la mise en œuvre de la stratégie.

On peut raccrocher à certains de ces thèmes (organisation du travail…) des facteurs de complexité qui favorisent des événements non souhaités :

Nombres de sites dont dispose l'organisme ;
Nombres d'organismes agréés de catégorie de classe A Partie-145 contractés ;
Nombre d'aéronefs en gestion ;
Nombre de type aéronefs en gestion ;
Organisme qui dispose des privilèges du CAMO.A.125(e) ;
Catégorie des aéronefs en gestion, complexité de la flotte ;
Organisme qui gère des aéronefs avec un régime d'exploitation spécifique ;
Organisme qui gère des aéronefs dont le programme d'entretien contient un programme de fiabilité ;
Exploitation sous CTA ou non des aéronefs en gestion ;
Organisme qui dispose des privilèges du CAMO.A.125(f) ;
Organisme qui sous-traite certaines tâches de gestion du maintien de la navigabilité ;
(…)

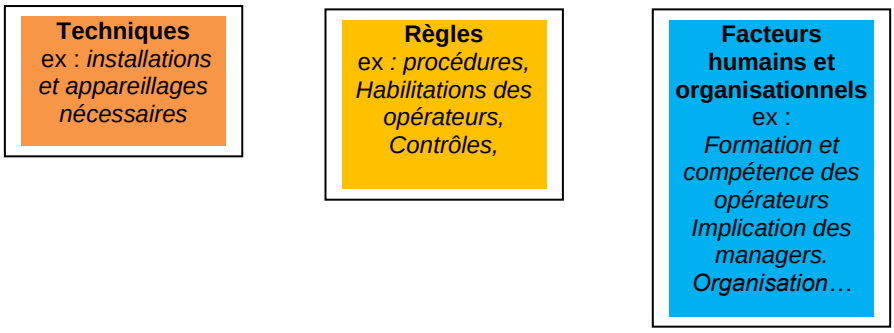
3.4.2.4. Le traitement du risque

Certains risques ont été évalués comme inacceptables. Ils doivent alors être traités. Ce type de traitement vise à réduire le risque à un niveau acceptable.

Comme le niveau de risque dépend de la vraisemblance d'occurrence d'un accident, et de la gravité des dommages, on cherchera donc à réduire leurs valeurs.

- On parle de **prévention** lorsque la vraisemblance d'occurrence d'un accident est réduite.
- On nomme **protection** un traitement réduisant la gravité des dommages.

Pour une situation donnée, **dont le risque est inacceptable**, plusieurs alternatives de **traitement** existent généralement. En pratique, plusieurs traitements sont souvent combinés.
Types de traitement :



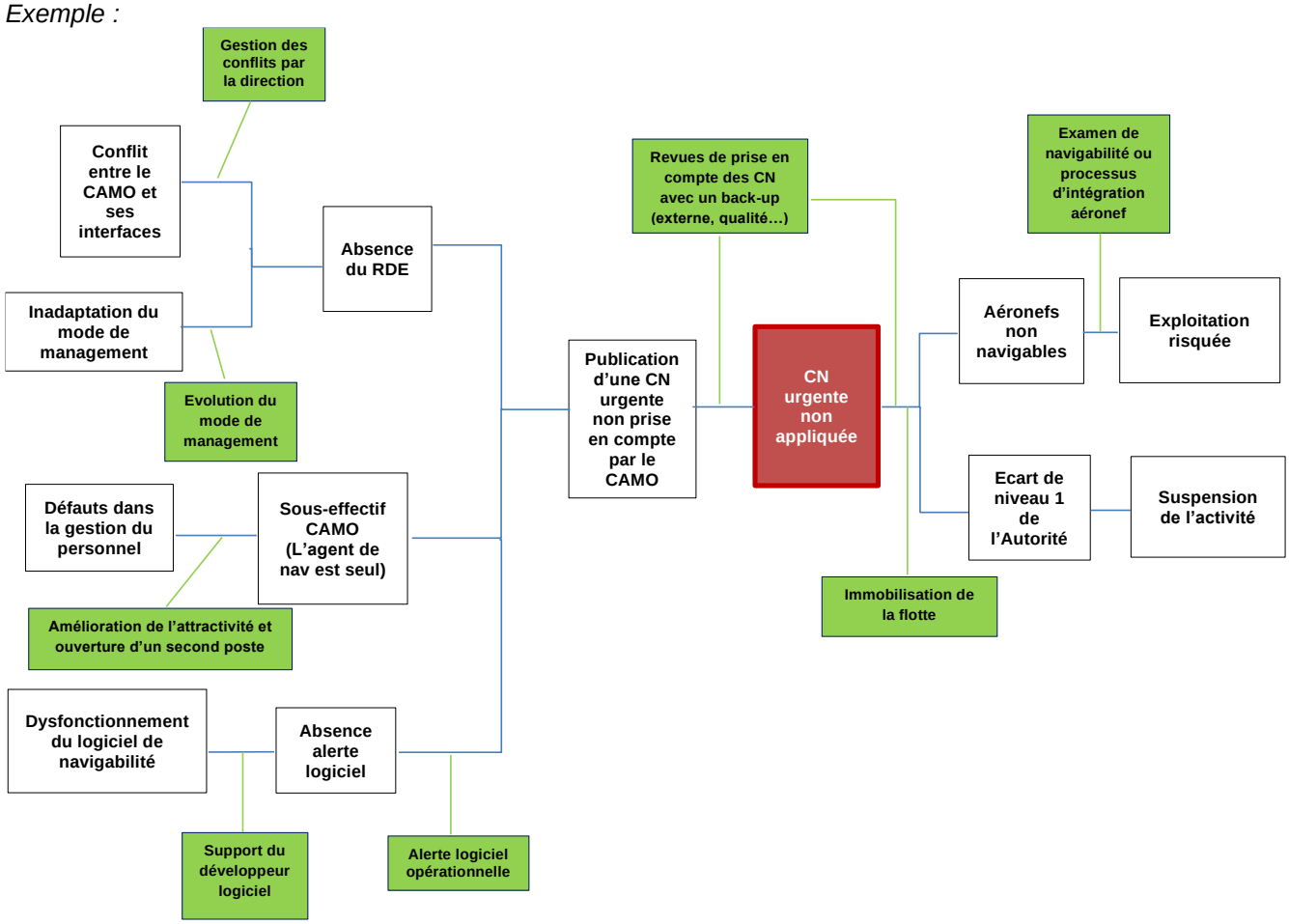
Ces traitements sont mis en œuvre par l'instauration de **barrières**. Ils doivent être faits en concertation entre les différents Responsables et le Dirigeant Responsable.

Des critères interviennent fréquemment pour effectuer ces choix :

- l'efficacité du moyen de traitement au regard de l'objectif de sécurité ;
- la fiabilité des barrières ;
- leur efficience, c'est-à-dire l'importance des ressources nécessaires à leur mise en œuvre.

Note : Les moyens de traitement des risques peuvent engendrer eux-mêmes de nouveaux risques qualifiés de **risques induits** : Il est indispensable d'itérer, c'est-à-dire d'identifier les risques induits puis d'en effectuer l'analyse et l'évaluation avant de proposer d'éventuels nouveaux traitements.

Exemple :



Le risque est réévalué après l'introduction des barrières.

Remarque : Cette évaluation est donnée à titre d'exemple et ne reflète pas la position de l'Autorité.

SITUATION DANGEREUSE	ÉVÉNEMENT INITIATEUR	PRÉVENTION	ÉVÉNEMENT REDOUTÉ	PROTECTION	CONSÉQUENCES	MAÎTRISE DU RISQUE	PROBABILITÉ	GRAVITÉ	ÉVALUATION ACCEPTATION
Réalisation de tâches de gestion du maintien de la navigabilité dans un environnement dysfonctionnel	Publication d'une CN urgente non prise en compte par le CAMO	**-Gestion des conflits** **- Evolution du mode de management** **-Amélioration de l'attractivité et ouverture d'un second poste** **-Support du développeur logiciel** **- Alerte logiciel opérationnelle** **- Revues de prise en compte des CN**	***Non application d'une CN urgente***	**- Revues de prise en compte des CN** **- Immobilisation de la flotte**	Aéronef non navigable	**BONNE**	**Faible (3)**	**Dangereux (B)**	**3B** **Tolérable**

Pour rappel le risque évalué initialement (avant introduction des barrières) était le suivant :

Probabilité	Gravité	ÉVALUATION ACCEPTATION
Occasionnel (4)	Catastrophique (A)	4A INTOLÉRABLE

- les barrières doivent rester **adaptées** pour être toujours **efficaces**. Leur suivi est donc essentiel ;
- **les barrières peuvent être affaiblies ou fragilisées par des perturbateurs :** l'organisation, le management, des procédures mal adaptées, les individus… ;
- **l'analyse de ces perturbateurs** issue du retour d'expérience, doit prévenir ces affaiblissements. Des parades sont mises en place.

Exemple d'évaluation et de gestion des barrières :

BARRIERES DE PREVENTION	PERTURBATEURS	PARADES	EFFICACITE PREVENTION	BARRIERES DE PROTECTION	PERTURBATEURS	PARADES	EFFICACITE PROTECTION	MAÎTRISE DU RISQUE
Alerte logicielle opérationnelle	- Panne du système - Règles de fonctionnement incomprises - (…)	-Remplacement du logiciel -Changement du prestataire -Formation du personnel -(…)	Bonne	Immobilisation de la flotte	- Pression de l'exploitation - (…)	- Vigilance de la direction sur la mise en œuvre de la stratégie de sécurité - Transmission de l'information à l'Autorité - (…)	Bonne	Bonne

A retenir :

Gérer et s'assurer de l'efficacité des barrières constitue une tâche primordiale pour le système de gestion.

L'organisme ne pouvant travailler sur tous les risques, l'attention doit être portée aux événements qui comportent un haut potentiel de gravité.

Attention à la dispersion des ressources ! Elles doivent être focalisées sur ce qui est important.

Le système de gestion et ses instances doivent développer et entretenir une conscience partagée des risques les plus importants.

Selon l'AMC1 CAMO.A.200(a)(3) §(b)(2), le niveau managérial qui a le pouvoir de prendre des décisions concernant l'acceptabilité des risques pour la sécurité doit être spécifié.

3.4.2.5. Comptes rendus d'événements en matière de sécurité

Références réglementaires	
AMC1 CAMO.A.200(a)(3) (c)	Safety management key process
CAMO.A.160	Compte rendu d'événements
AMC1 et AMC 2 CAMO.A.160	Occurrence reporting
CAMO.A.202	Dispositif interne de compte rendu
AMC1 CAMO.A.202	Internal safety reporting scheme

3.4.2.5.1. L'enquête interne

Conformément à sa politique de culture juste, l'organisation enquête sur des incidents tels que des erreurs ou des quasi-accidents, afin de comprendre non seulement ce qui s'est passé, mais également comment est-ce arrivé.

Il s'agit ici de décider et de mettre en œuvre des mesures de prévention ou de protection afin de réduire la probabilité et / ou les conséquences de récurrences futures.

En s'interrogeant sur « comment est-ce arrivé » ? il faut à partir des causes immédiates, remonter aux causes plus profondes (organisationnelles ou techniques) qui ont conduit à l'événement comme :

- la nature des défaillances techniques ;
- l'organisation du travail ;
- la formation ;
- la gestion des ressources humaines ;
- les interactions ;
- la documentation ;
- la qualité du management ;
- la collaboration entre les acteurs ;
  (…)

Exemple relatif à la non prise en compte d'une consigne de navigabilité. Qu'est-ce qu'il y avait dans l'organisme pour que la situation de travail soit dégradée, pour que le responsable ne voit pas l'alerte, pour que le collectif ne récupère pas la situation ? Les procédures sont-elles adaptées ? Quel est le style managérial de la direction ? Quelles sont les relations entre le RD, le DR ou le RSC ?

Il faut s'intéresser aux événements où l'on est passé près de quelque chose de grave.
Se prévenir des événements les plus graves, c'est aussi s'intéresser aux événements qui se sont bien terminés mais qui ont un haut potentiel de gravité.

Attention ! Des événements récurrents ont une signification sous-jacente importante. Ils prouvent que les risque sont insuffisamment pris en compte, tant dans leur évaluation que dans leur traitement.

Il y a là un signal d'une problématique de sécurité latente qui pourrait avoir des conséquences plus graves si elle perdure.

Il doit y avoir deux types de traitement lors d'événements :

- la recherche des causes profondes (techniques et organisationnelles) avec les personnes compétentes ;
- le traitement individuel avec les personnes impliquées dans l'événement dans le cadre d'une politique de culture juste.

3.4.2.5.2. Les comptes rendus d'événements

Dans le cadre de son système de gestion, l'organisation doit mettre en œuvre un système de compte rendu d'événements obligatoire et volontaire conforme aux exigences définies dans le règlement **(UE) n°376/2014** et le règlement d'exécution **(UE) 2015/1018**. Ce compte rendu doit être produit sous une forme et d'une manière établie par l'autorité compétente.

Le règlement (UE) n°376/2014 décrit les exigences pour les organismes en termes de notification à l'autorité, d'analyse et de suivi des événements de sécurité.
Un livret explicatif (https://www.ecologie.gouv.fr/sites/default/files/guide_notifier_incident_0.pdf) complet et pédagogique produit par la DSAC explique les exigences réglementaires et les bonnes pratiques en la matière.

Selon le CAMO.A.160 et l'AMC2 CAMO.A.160, l'organisme veille à rendre compte à l'autorité compétente et à l'organisme responsable de la conception de l'aéronef de l'ensemble des incidents, défaillances, défauts techniques, dépassements des limitations techniques, événements qui mettraient en évidence des informations inexactes, incomplètes ou ambiguës contenues dans les données établies conformément à l'annexe I (partie 21) du règlement (UE) n°748/2012, et de toute autre circonstance anormale qui a ou est susceptible d'avoir compromis l'exploitation sans risque de l'aéronef, mais qui n'a pas donné lieu à un accident ou à un incident grave.
Ce dernier pourra émettre des recommandations appropriées à tous les propriétaires ou exploitants.

Selon le CAMO.A.202 l'organisme doit toujours :

- donner accès à son système interne de rapports de sécurité à toute organisation sous-traitante ;
- coopérer en matière d'enquêtes de sécurité avec tout autre organisme ayant une contribution significative à la sécurité de ses propres activités de gestion du maintien de la navigabilité (le propriétaire, l'exploitant…).

Selon l'AMC 1 CAMO.A.202 le schéma de report interne devrait :

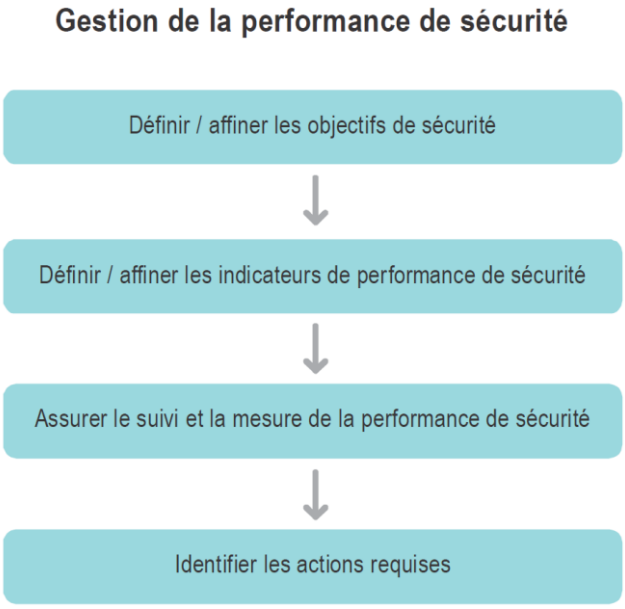
- pouvoir établir tous les facteurs de causalité et contributifs, y compris tous les problèmes techniques, organisationnels, de gestion ou humains, et tout autre facteur contributif lié à l'événement ;

- (Si adapté à la taille et à la complexité de l'organisation), analyser les données collectives montrant les tendances et les fréquences des facteurs contributifs ;
- comporter formation initiale et périodique du personnel impliqué dans les enquêtes ;
- contribuer à la formation périodique tout en maintenant une confidentialité appropriée ;
- définir les éventuelles actions correctives pouvant être mises en place (« boucle courte »).

3.4.2.6. Surveillance et mesure de la performance de sécurité

Références réglementaires	
AMC1 CAMO.A.200(a)(3) (d)	Safety management key process

3.4.2.6.1. Généralités



Source OACI

La gestion de la sécurité permet de rendre le risque acceptable. On pourrait donc estimer lors du déroulement de l'activité que « tout est sous contrôle ».
Or cette affirmation est fausse si les **objectifs prioritaires** en matière de sécurité ne sont pas mis en œuvre de **manière effective** à travers des actions.

La notion de surveillance implique celle de pilotage.

Exemple :

Un plan d'actions prioritaires a été défini dans le cadre de la surveillance de la réalisation des objectifs.
Il formalise successivement dans un tableau :
-les objectifs prioritaires ;
-leur déclinaison en actions prioritaires ;
-leur répartition en termes de porteur d'action ;
-leur répartition dans le temps.

Cet outil ainsi construit aide les différents responsables dans le pilotage de la performance de sécurité.

Les SRB sont des occasions pour assurer la surveillance de la performance. Elle doit cependant faire partie des actions de pilotage continues de l'encadrement du Système de Gestion.

La définition de la stratégie de sécurité avec ses objectifs associés, et la surveillance de sa bonne mise en œuvre peut s'appuyer sur diverses sources d'information :

- la remontée d'événements et leur analyse ;
- les études de sécurité dont celles portant sur des dysfonctionnements les activités quotidiennes de gestion du maintien de la navigabilité ou sur la coopération au sein de l'organisme ;
- la gestion des changements pouvant affecter la sécurité comme l'introduction de nouveaux équipements / technologies, la mise en œuvre de procédures nouvelles ou modifiées ou dans des situations de changements organisationnels ;
- les résultats des audits du système de gestion ;
- le suivi de l'ensemble des actions correctives et préventives et l'évaluation de leur efficacité ;
- le suivi des objectifs et des actions associées ;
- le suivi des indicateurs de sécurité et de conformité ;
- etc.

3.4.2.6.2. La définition et le suivi des indicateurs

1/ Généralités

Un indicateur est une **mesure**. Il mesure des informations liées aux **objectifs à atteindre** : *est-il atteint ?*
Il peut également être considéré comme un concentré d'informations qui **stimule l'action** (exemple, un plan d'actions prioritaire).

Il peut être de nature :

- **Réactive**, utilisé pour enquêter ou analyser des défaillances *(exemple : nombre d'événements de sécurité liés à la non prise en compte d'une directive de navigabilité).*
  Il traduit souvent les résultats négatifs que l'organisation vise à éviter.
- **Proactive**, pour vérifier que les actions d'anticipation sur des points de sécurité sont menés dans de bonnes conditions *(exemple : nombre de personnes formées au SGS).*
  Il surveille les mesures mises en œuvre pour améliorer ou maintenir le niveau de sécurité.

et

- **Quantitatif** : Il porte sur des éléments qui peuvent être chiffrés et s'exprime par un chiffre ou par un taux.
- **Qualitatif :** Il décrit la qualité du résultat *(exemple : mise en place d'une documentation ou d'une procédure spécifique ou encore qualité d'un comportement).*

2/ Les étapes de mise en place des indicateurs

A/ Définir des objectifs généraux (stratégiques) internes

B/ Les objectifs sont déclinés en objectifs intermédiaires de plus bas niveau : Des valeurs à atteindre peuvent être définies.

C/ Définir des critères d'évaluation (que mesure-t-on) ? : Il s'agit de repérer les informations liées aux actions de mise en œuvre de la stratégie. Si l'on reste au niveau des objectifs stratégiques, les indicateurs seront trop vagues.

D/ Sélectionner et mettre en forme des indicateurs : Une fois les critères établis (« le quoi ») se pose la question du « comment ». Comment peut-on effectuer une mesure pour chacun des critères retenus ? Il faut ici les nommer et choisir au besoin des unités de mesure.

E/ Evaluer et faire évoluer les indicateurs : Les objectifs et indicateurs doivent être remis à jour régulièrement ou lors de changements éventuels.

Exemple relatif à l'implication du personnel dans un organisme :

Objectif Général	Améliorer l'implication des Responsables Désignés (RD) dans la gestion de la sécurité				
Objectifs intermédiaires	Améliorer l'implication des RD dans l'analyse et l'exploitation des comptes rendus d'événements (CRES)		Améliorer la participation des RD en SRB sur les problématiques de sécurité		Systématiser la présentation et l'évaluation des mesures de sécurité dans les réunions de travail avec les équipes
Critères d'évaluation	Participation des RD aux analyses des CRES	Mise en œuvre des actions de sécurité	Remontée des problématiques de sécurité du domaine des RD en SRB	Bilan de l'efficacité des actions de sécurité par les RD	Effectivité de cette prise en compte
Valeur à atteindre	80 %	100%	Qualitative	100%	Qualitative
Indicateurs	Nombre d'analyses réalisées par les RD / nombre de CRES x 100	Pourcentage d'actions correctives effectivement mises en place	Remontée à chaque SRB	Nombre de actions de sécurité évaluées / nombre décidées x 100	Intégration des points à l'ordre du jour

Rappel :

- Les objectifs doivent identifier les porteurs d'actions et décrire les actions à mener pour les atteindre (ou objectifs spécifiques).
- Les indicateurs devraient être reliés au tableau de bord de chaque pilote d'actions prioritaires.

3.4.2.7. La gestion des changements

Références réglementaires	
AMC1 CAMO.A.200(a)(3) (e)	Safety management key process
Se référer également au CAMO.A.130 et au guide G-48-00	

La gestion du changement est une **étude de sécurité** couplée à un **plan d'actions** dont les porteurs sont identifiés. Elle implique les principales parties prenantes.

L'objet ici est de matérialiser les conséquences internes relatives à un changement temporaire ou permanent : **quels événements peuvent survenir à cette occasion et quelle serait leurs gravités ?** Des barrières doivent ainsi être mises en place d'une manière cadencée selon l'avancée du changement et de façon proportionnelle au potentiel de gravité.
L'aspect FOH doit également être pris en compte pour évaluer l'impact du changement sur les personnes au sein d'un système.

Points clés :

- le processus de gestion du risque doit être appliqué ;
- une étude de conformité doit être menée : le changement respecte-t-il les exigences réglementaires ?
- de par la récurrence des changements, c'est une procédure à mettre en place au sein de l'organisme ;
- elle inclut des mesures de suivi permettant de vérifier que le changement a été effectué de manière sûre.

Pour chaque changement devant donner lieu à une étude de sécurité, l'exploitant peut se poser les questions suivantes :

- Un changement similaire a-t-il déjà fait l'objet d'une évaluation d'impact sur la sécurité ?
- Quels sont les événements indésirables ? (En tenant compte des spécificités du changement considéré).
- Les événements indésirables identifiés sont-ils les mêmes ?

- ➢ Les mesures en réduction de risque identifiées dans l'étude précédente sont-elles toujours pertinentes et applicables ?

Remarques sur les manques fréquents :

- l'un des deux aspects (Conformité/Sécurité) n'est pas couvert ;
- le plan d'actions ;
- le suivi des actions ;
- l'assurance que les actions nécessaires sont mises en place avant le changement.

Voici quelques exemples de changements :

- modifications de la structure organisationnelle ;
- l'inclusion d'un nouveau type d'aéronef dans les conditions d'approbation ;
- l'ajout d'aéronefs du même type ou d'un type similaire ;
- changements importants dans le personnel (affectant le personnel clé et / ou un grand nombre de personnel, taux de roulement élevé) ;
- règlements nouveaux ou modifiés ;
- les modifications des dispositions de sécurité ;
- changements dans la situation économique d'une organisation (par exemple, pression commerciale ou financière) ;
- nouveaux horaires, nouveaux emplacements, équipements et / ou procédures opérationnelles ;
- l'ajout de nouveaux sous-traitants.

3.4.2.8. L'amélioration continue

Références réglementaires	
AMC1 CAMO.A.200(a)(3) (f)	Safety management key process

Ce thème prolonge la partie sur la gestion de la performance de sécurité abordée au §3.4.2.6.

L'organisme doit constamment chercher à améliorer ses performances en matière de sécurité et d'efficacité de son système de gestion et à réduire ses dysfonctionnements.
Le Système de Gestion ne peut être efficace que si les dysfonctionnements de l'organisation sont limités.

L'amélioration continue peut s'appuyer sur :

- la **surveillance de la conformité** et de l'efficacité effectués par des audits qui apporte au Dirigeant Responsable et aux membres du SRB des informations sur le système de gestion ;
- les **enquêtes** auprès du personnel qui peuvent fournir des informations utiles sur l'implication des personnes dans le système de gestion ;
- la **surveillance de la récurrence** des événements et des incidents ;
- **l'évaluation des indicateurs** de performance de sécurité ;
- les **facultés d'apprentissage** de l'organisation.

Sur la base des résultats obtenus, il convient de prendre des décisions sur les possibilités d'amélioration du cadre organisationnel, de la stratégie et de la gestion des risques.

Ces décisions entraînent des améliorations de la culture de sécurité au travers de l'implication des individus et de leurs actions concrètes.

3.4.2.9. L'emergency response plan (ERP)

Références réglementaires	
AMC1 CAMO.A.200(a)(3) (g)	Safety management key process

Une organisation doit agir rapidement lorsqu'elle a identifié des problèmes susceptibles d'avoir un effet imminent sur la sécurité des vols, c'est l'objet de **l'Emergency Response Plan établi par l'exploitant de l'aéronef.**

L'organisme doit s'assurer d'être associé aux exercices périodiques de mise en œuvre du plan de l'exploitant.

Dans le cadre d'un CAMO, une problématique de navigabilité majeure nécessite une **information immédiate auprès du propriétaire de l'aéronef ou de l'exploitant.**

Les coordonnées de ces contacts doivent être **accessibles facilement et mises à jour**. Elles permettent une **communication en dehors des heures ou jours ouvrables.**

Dans le cas où un exploitant déclencherait son plan de gestion de crise interne (ERP), le Responsable Désigné de l'organisme de gestion de la navigabilité devra apporter son soutien selon le plan établi.

Ainsi il peut par exemple :

- Dresser une liste des documents administratifs relatifs à la maintenance de l'aéronef impliqué dans l'accident et au maintien de sa navigabilité (Certificat d'immatriculation, Certificat de navigabilité, Certificat d'examen de navigabilité, fiche matricule équipement, livret moteur, etc.), ainsi que tous les enregistrements de l'entretien réalisé sur l'aéronef et ses systèmes, et les met à disposition des autorités chargées de l'enquête ;
- Aider les autorités chargées de l'enquête avec l'expertise technique sur demande.

3.5. Maintien des compétences des personnels

Références réglementaires	
CAMO.A.200(a)(4)	Maintien des compétences
AMC1 CAMO.A.200(a)(4)	Communication on safety

3.5.1. La promotion de la sécurité

La promotion de la sécurité participe à la culture de la sécurité positive en ce sens qu'elle favorise le partage des manières de faire et de penser à propos des risques les plus importants de l'organisation.

Elle complète les politiques et processus de l'organisme en maintenant la conscience du risque des personnels.

Elle concourt également à l'atteinte des objectifs de sécurité par l'augmentation des compétences techniques à travers la formation, la sensibilisation.

Deux piliers sont utilisés.

3.5.1.1. La formation

L'organisme doit s'assurer que son personnel est formé et compétent pour effectuer ses tâches.
Pour cela, il établit un plan de formation initiale et continue, et s'assure que ses sous-traitants font de même pour leurs employés.
Les actions de formation ne sont pas menées uniquement à l'arrivée de nouveaux personnels.

En matière de Gestion de la sécurité, le plan de formation contient au minimum :

- une **formation initiale** :
  - **sensibilisation** aux principes de la gestion de la sécurité, pour tous les personnels dont l'activité peut avoir un impact sur la sécurité ;
  - **formation plus approfondie**, pour les agents directement impliqués dans la gestion de la sécurité, par exemple au cadre responsable, aux responsables désignés, au responsable de gestion de la sécurité, au responsable de surveillance de la conformité, aux correspondants sécurité, mais également à certains agents opérationnels ;
- une **formation continue** pour entretenir les compétences ainsi acquises.

En matière de Surveillance de la conformité, le plan de formation contient au minimum :

- une **formation initiale :**
  - **sensibilisation** aux principes de la conformité, pour tous les personnels dont l'activité peut avoir un impact sur la sécurité ;
  - **formation plus approfondie**, pour les agents directement impliqués dans la surveillance de la conformité, par exemple au dirigeant responsable, aux responsables désignés, au responsable de la gestion de la sécurité, au responsable de surveillance de la conformité, aux auditeurs.
- une **formation continue** pour entretenir les compétences ainsi acquises.

La **sensibilisation Gestion de la sécurité et Surveillance de la conformité** peut porter sur :

- la réglementation du système de gestion ;
- l'organisation du système de gestion au sein de l'organisme, et son fonctionnement ;
- les objectifs de sécurité et de conformité ;
- le rôle de chacun dans le système de gestion ;

- la notification d'événements ;
- les facteurs humains ;
- le programme de surveillance de la conformité ;
- etc.

La **formation Gestion de la Sécurité plus approfondie** devrait couvrir notamment :

- l'analyse des événements ;
- la gestion des risques (dont utilisation du modèle de risque) ;
- la conduite d'une étude de sécurité systémique ou en cas de changement ;
- le lien avec la Surveillance de la Conformité ;
- etc.

La **formation Surveillance de la Conformité plus approfondie** devrait couvrir notamment :

- le concept de conformité ;
- l'encadrement du système de gestion ;
- le concept de l'assurance de la conformité ;
- les manuels et procédures relatifs aux tâches des personnes concernées ;
- les techniques d'audit ;
- les comptes rendus et le système d'enregistrements ;
- et la façon dont le système de gestion fonctionne précisément dans l'exploitant ;
- le lien avec la Gestion de la Sécurité ;
- etc.

Il est important d'incorporer à la formation le retour d'expérience issu de l'activité. Il constitue un socle de connaissance très riche.

Au sein d'un organisme, l'instauration d'une réflexion collective sur les solutions à apporter à des problématiques rencontrées permet d'améliorer sa capacité à affronter les sujets complexes et sa capacité d'apprentissage.

3.5.1.2. La communication

Elle porte sur la diffusion de la politique de sécurité avec ses objectifs et de toute autre information pertinente comme des informations concernant les risques évalués et les dangers analysés.

Elle participe à ce que tout le personnel connaisse les enjeux de sécurité relatifs à son domaine d'activité et de responsabilité ainsi que le fonctionnement du système de gestion.

Elle a une vertu pédagogique en ce sens qu'elle explique pourquoi des procédures de sécurité sont introduites ou modifiées ou des actions sont prises.

Les supports possibles sont multiples : note sécurité, mail, revues, réunions…

Des réunions régulières avec le personnel au cours desquelles des informations, des actions et des procédures sont discutées peuvent être utilisées pour communiquer sur les questions de sécurité.

L'organisme veille à ce que l'information transmise soit pertinente et stimulante.

3.6. Documentation

Références réglementaires	
CAMO.A.200 (a)(5)	Documentation
GM1 CAMO.A.200 (a)(5)	Management system

L'organisme documente sa politique de sécurité, ses objectifs de sécurité et tous les processus clés de son système de gestion soit dans un manuel séparé (par exemple, le manuel de gestion de la sécurité ou le manuel du système de gestion) ou soit dans son CAME (cf. AMC1 CAMO.A.300, partie 2). « Procédures du système de gestion »).

Les organisations qui détiennent plusieurs certificats selon le règlement (UE) 2018/1139 peuvent préférer utiliser un manuel séparé afin d'éviter les doublons. Ce manuel ou le CAME, selon les cas, doit être l'instrument clé pour communiquer l'approche du système de management pour l'ensemble de l'organisation.

L'organisme peut également choisir de documenter certaines informations dans des documents distincts (par exemple, documents de politique, procédures). Dans ce cas, il doit s'assurer que le manuel ou le CAME contient

des références adéquates à tout document conservé séparément. Ces documents doivent être considérés comme faisant partie intégrante de la documentation du système de gestion de l'organisation

3.7. Contrôle de la conformité

Références réglementaires	
CAMO.A.200(a)(6)	Contrôle de la conformité
AMC1 CAMO.A.200(a)(6)	General
AMC2 CAMO.A.200(a)(6)	Independant audit
AMC3 CAMO.A.200(a)(6)	Compliance monitoring
AMC4 CAMO.A.200(a)(6)	Feedback system

3.7.1. La fonction de surveillance de la conformité, une approche en deux phases

Le rôle dévolu au responsable de la surveillance de la conformité (RSC) est double. Il doit vérifier :

- que les activités de l'organisme sont surveillées pour s'assurer qu'elles sont conformes aux exigences réglementaires applicables et aux exigences additionnelles établies ;
- que ces activités sont correctement menées sous la supervision d'un responsable (RDE/RDMN).

Par conséquent la surveillance interne de la conformité est une approche en deux phases. Il s'agit :

- dans la première phase, d'établir des procédures qui garantissent que les exigences réglementaires sont transcrites au sein de l'organisme et placées sous la responsabilité d'un responsable ; 1
- dans la seconde phase, de s'assurer que ces procédures sont suivies au travers d'une supervision au quotidien par le management de proximité ainsi qu'au travers d'une surveillance régulière sous forme d'audits et inspections indépendants des processus. 2

1. Phase 1

Dans cette phase, l'organisme transpose les normes (exigences réglementaires, etc…) dans des procédures. Cette démarche consiste non pas en une recopie des normes mais en la description de la façon dont l'exploitant entend que son personnel effectue ses tâches.
Les procédures sont établies par la personne responsable du processus.

A l'issue de cette première phase l'organisme dispose ainsi :

- de **Procédures**, c'est-à-dire d'une description claire pour ses personnels de la façon dont l'organisme attend qu'ils travaillent ;
- d'une **Grille (ou « matrice ») de conformité** (table de références croisées), démontrant que toutes les exigences applicables ont bien été prises en compte par *(transposées dans)* les procédures appropriées.

La **grille de conformité**, est donc l'outil pour :

- **démontrer** la conformité dans le processus de **certification ;**
- **identifier** les procédures à modifier lorsque les **normes** sont **amendées.**

Exemple de grille de conformité :

Exigence		**Référentiel Exploitant**	**Commentaires**
Règle N	AMC1 § 1 à 2	CAME part 2.2	
	AMC1 § 3 à 4	CAME part 2.6	
Règle N+2		Procédure SG n°xx	
Règle N+3		Manuel SG section 2.3	
etc		etc	

2. Phase 2

Cette phase consiste pour l'organisme à s'assurer que les procédures sont suivies.
La conformité de l'exploitation aux procédures relève, en premier lieu, de la responsabilité au quotidien des managers/superviseurs sous la responsabilité ultime des responsables dans le cadre de leur activité de supervision.

Elle fait, en second lieu dans le cadre de la surveillance de la conformité, l'objet d'une vérification interne indépendante, aux moyens d'audits et de contrôles. Celle-ci :

- commence par la grille de conformité, en faisant référence aux normes applicables qui ont été transposées, ce qui permet d'identifier les procédures qui entrent dans le périmètre de l'audit ;
- puis consiste à vérifier que les procédures sont suivies, non pas en se référant aux normes mais en se référant aux détails décrits dans le référentiel de l'organisme.

3. Synthèse des deux phases

La synthèse des phases 1 et 2 peut ainsi se faire au moyen d'un outil « Matrice (ou grille) de conformité ». La forme de cet outil n'est pas imposée, mais il devrait en revanche répondre aux objectifs suivants :

1 **Exhaustivité :** L'outil utilisé doit permettre de démontrer facilement de façon synthétique que l'ensemble des exigences réglementaires applicables a bien été pris en compte dans la **phase 1**.

2 **Surveillance :** En combinant les deux phases, l'outil permet de construire un **programme** de surveillance **exhaustif** et **efficace** et des **check-lists** pertinentes.

1+2 **Assurance de la conformité :** Si l'outil est renseigné avec les résultats des actes de surveillance ainsi réalisés, il permet à l'organisme d'avoir une image précise et à jour de sa conformité.

Maintien de la conformité – Gestion des Changements : L'utilisation de l'outil permet de faciliter et de documenter l'étape « **étude d'impact sur le maintien de la conformité** » lors de la **gestion des changements.**

3.7.2. Exigences

Les principaux objectifs de la surveillance de la conformité sont de fournir une fonction de surveillance indépendante sur la façon dont l'organisation garantit la conformité aux exigences, politiques et procédures applicables, et de demander des mesures en cas de non-conformité.

L'indépendance du contrôle de la conformité doit être établie en veillant toujours à ce que les audits et inspections soient effectués par du personnel qui n'est pas responsable des fonctions, procédures ou produits audités ou inspectés.
Cette indépendance permet de fournir à l'exploitant un regard extérieur lui permettant d'évaluer de façon objective la conformité de ses opérations.

La fonction de surveillance de la conformité doit être adaptée à la taille de l'exploitant ainsi qu'à la complexité de ses activités.
La description de l'organisation et du fonctionnement de cette fonction doit être documentée.

3.7.3. Modalités

Il existe deux types d'actes de surveillance, les audits et les inspections (ou « contrôles »).

A/ Inspection (ou « contrôle »)

Une inspection est une évaluation indépendante et documentée de la conformité par l'observation et le jugement assortie le cas échéant de mesures, d'essais, afin de vérifier la conformité aux exigences applicables.

B/ Audit

Un audit est un processus systématique, indépendant et documenté permettant d'obtenir des preuves et d'évaluer de manière objective en vue de déterminer dans quelle mesure des exigences sont respectées.

Les audits devraient comporter au moins les procédures qualité et procédés suivants :

- une définition de l'objet de l'audit ;
- la planification et la préparation ;
- le rassemblement et l'enregistrement des preuves ;
- l'analyse des preuves.

Les techniques d'audit comprennent :

- des entrevues ou discussions avec le personnel ;
- une revue des documents produits par l'entité auditée ;
- l'examen d'un échantillon adéquat d'enregistrements ;
- l'observation des activités qui constituent l'exploitation ;
- la conservation des preuves récupérées ;
- l'enregistrement des observations (utilisation de check-list d'audit).

3.7.4. Auditeurs et autres acteurs de la surveillance de la conformité

Le RSC peut choisir de réaliser tous les audits seul ou de faire appel à un ou plusieurs auditeurs, en interne ou en externe.

Si du personnel externe est utilisé pour effectuer des audits indépendants :

- ces audits sont effectués sous la responsabilité du responsable du contrôle de la conformité ;
- l'organisme demeure responsable de s'assurer que le personnel externe possède les connaissances, les antécédents et l'expérience appropriés aux activités auditées, y compris les connaissances et l'expérience en matière de surveillance de la conformité ;
- l'organisme conserve la responsabilité ultime de l'efficacité de la fonction de contrôle de la conformité, en particulier de la mise en œuvre et du suivi efficaces de toutes les actions correctives.

Les qualifications et les responsabilités des auditeurs devraient être clairement définies dans la documentation pertinente.
L'organisme devrait tenir à jour une liste des auditeurs et des contrôleurs.

3.7.5. Programme de surveillance interne

La fonction de surveillance de la conformité s'organise autour d'un programme de surveillance annuel qui comprend la planification d'audits selon un cycle périodique. Le principe est de déterminer quand et à quelle fréquence les activités requises par les parties M, ML et CAMO seront auditées.

Tous les aspects de la conformité sont vérifiés sur la durée d'un cycle (12 mois), y compris toutes les activités sous-traitées.

Notes :

- En l'absence de constatations relatives à la sécurité, les durées de cycle de planification de l'audit peuvent être augmentées jusqu'à 100% (24 mois) sous réserve d'une évaluation des risques appropriée et d'un accord de l'autorité compétente.

- Une procédure commune à plus d'une ligne de produits qui est vérifiée annuellement sans constat sur une ligne permet un allègement de la surveillance sur les autres lignes.
  En revanche, lorsque des constatations ont été identifiées, la procédure concernée doit être vérifiée par rapport à d'autres gammes de produits jusqu'à ce que les constatations soient corrigées, après quoi il est possible de revenir à l'intervalle annuel pour la procédure en question.
- Lorsque l'organisation a plus d'un site approuvé, le plan d'audit doit garantir que chaque site est audité chaque année ou à un intervalle déterminé par une évaluation des risques convenue par l'autorité compétente et ne dépassant pas le cycle de planification d'audit applicable.

3.7.6. Système de retour d'informations

Un élément essentiel de la surveillance de la conformité est le système de retour d'informations.
Il permet de veiller à ce que toutes les constatations résultant des audits indépendants soient correctement examinées et corrigées en temps opportun, et de tenir le DR informé de tout problème de sécurité d'une part et du degré de conformité d'autre part.

Ce système de retour d'information ne devrait pas être confié à des personnes ou des organisations externes à moins qu'il soit associé à l'externalisation de la fonction RSC.

Lorsqu'une non-conformité est constatée, la fonction de surveillance de la conformité doit établir :

- le niveau de sévérité de la constatation (ex : écart majeur, écart, remarque) et le délai approprié de réponse qu'il convient d'apporter (ex : besoin d'une action corrective immédiate pour un écart majeur) ;
- l'origine de la constatation (cause racine) ;
- les actions correctives nécessaires pour s'assurer que la non-conformité ne se reproduise pas ;
- une programmation des actions correctives ;
- l'identification des départements et personnes en charge de la mise en œuvre des actions correctives.

Les rapports d'audit indépendants mentionnés dans AMC2 CAMO.A.200 (a) (6) doivent être envoyés au (x) service(s) compétent(s) pour action corrective, avec indication des dates de clôture.

Ces dates cibles doivent être discutées avec le(s) département(s) concerné(s) avant que la fonction de surveillance de la conformité ne confirme les dates dans le rapport.

Le ou les services concernés sont tenus de mettre en œuvre l'action corrective et d'informer la fonction de contrôle de la conformité de l'état de la mise en œuvre de l'action.

Pour les organismes de petite taille ne disposant pas de cette instance de gouvernance, le Dirigeant Responsable doit tenir des réunions régulières avec le personnel pour vérifier l'état d'avancement des actions correctives.

Cette gestion peut être déléguée au **Responsable de la Surveillance de la Conformité**, sous réserve que :

1) le Cadre Responsable se réunisse au moins **deux fois par an** avec les **Responsables Désignés** concernés pour examiner la performance globale ; et
2) qu'il reçoive au moins un **rapport** semestriel sur les constatations de non-conformité.

Constatations notifiées par l'Autorité

CAMO.A.150

Les constatations de niveau 1 ou 2 notifiées par l'Autorité doivent être prises en compte par l'exploitant au travers de sa fonction de surveillance de la conformité.

L'organisme doit :

1) déterminer le ou les faits qui y ont donné lieu et les facteurs qui contribuent au non-respect ;

2) définir un plan d'actions correctives ;

3) prouver, à la satisfaction de l'autorité compétente, la mise en œuvre de l'action corrective.

Les actions visées aux points a) 1), a) 2) et a) 3) sont mises en œuvre dans les délais convenus avec cette autorité.

3.8. Exigences supplémentaires – contrats et contrats de sous-traitance

Références réglementaires	
CAMO.A.200 (a)(7)	Documentation
CAMO.A.205	Contrats et contrats de sous-traitance
GM1 CAMO.A.205	Contracting and subcontracting

L'organisme s'assure que, lorsqu'il passe un contrat de maintenance (« contracting » dans la version anglaise) ou un contrat de sous-traitance (« subcontracting » dans la version anglaise) concernant une partie quelconque de ses activités de gestion du maintien de la navigabilité :

1) ces activités respectent les exigences applicables ;
2) tous dangers pour la sécurité aérienne liés à ce contrat ou contrat de sous-traitance sont pris en compte dans le système de gestion de l'organisme.

Lorsque l'organisme donneur d'ordre sous-traite une partie de ses activités de gestion du maintien de la navigabilité à un autre organisme (agréé ou non), cet autre organisme sous-traitant travaille sous couvert de l'agrément de l'organisme donneur d'ordre. L'organisme donneur d'ordre veille à ce que l'autorité compétente ait accès à l'organisme sous-traitant, afin de déterminer le maintien de la conformité avec les exigences applicables.

La sous-traitance introduit pour le donneur d'ordre un risque de défaut de surveillance du sous-traitant et de perte de maîtrise de la conformité des produits et activités réalisés par le sous-traitant.
En conséquence, le donneur d'ordre doit mettre en place des mécanismes de maîtrise de ce risque et une surveillance efficace du sous-traitant.

La surveillance de la conformité doit vérifier que le domaine d'agrément de l'organisme de maintenance couvre effectivement les activités contractées et qu'il est toujours valide.

Un CAMO est responsable de s'assurer qu'un système de communication est établi avec l'organisme de maintenance contracté en ce qui concerne les rapports d'incident.
Cela n'exonère pas l'organisme contracté de son obligation de faire un rapport à l'autorité compétente conformément au règlement (UE) n°1321/2014.

Pour les activités sous-traitées, l'organisme donneur d'ordre doit toujours donner accès à son système interne de rapports de sécurité à toute organisation sous-traitante selon les dispositions du CAMO.A.202.

4. ANNEXE

L'approche organisationnelle des systèmes de gestion

D'après l'OACI, *« la gestion de la sécurité doit aborder la manière dont les humains contribuent, tant positivement que négativement, à la sécurité de l'organisation »*. Elle mentionne par ailleurs la notion de facteurs organisationnels en prenant en considération l'incidence de la culture et des politiques organisationnelles sur l'efficacité de la maîtrise des risques de sécurité. L'EASA ajoute que *« le comportement humain est influencé par l'environnement organisationnel »* (GM1 CAMO.A.200).

4.1. Les composantes d'une organisation : schémas généraux

Un système de gestion permet de contrôler les risques de non-conformité et de sécurité en mettant en œuvre des fondamentaux tels que :

- Une gouvernance active et convaincue ;
- Le respect des protocoles et leur mise à jour en fonction du retour d'expérience ;
- Le développement de stratégies permettant de gérer ou d'anticiper les défaillances, les erreurs, les aléas et leurs conséquences ;
- Le traitement des erreurs et des violations ;
- (…)

Or l'effectivité et l'efficacité de cette mise en œuvre dépend de la qualité même du fonctionnement de l'organisation, de la cohésion entre ses membres. Cette dernière peut être résumée comme un ensemble humain structuré se donnant des objectifs.

A/La structuration

La structuration de cet ensemble a les caractéristiques suivantes :

- Division des tâches ;
- Distribution des rôles ;
- Supervision d'un système d'autorité ;
- Utilisation d'un système de communication ;

➢ La gestion de la sécurité doit donc bénéficier de la structuration de l'organisation. Elle est décrite par la réglementation.

B /La définition des objectifs

De la stratégie découle la formalisation des objectifs. Ils s'appuient sur des ressources :

- Humaines (compétences, temps, énergie) ;
- Matérielles ;
- Financières ;
- Informationnelles ;
- ….

➢ La gestion de la sécurité nécessite de définir des objectifs propres à la sécurité et à la conformité en bénéficiant de ressources.

C/ L'atteinte des objectifs

Les différentes ressources évoquées doivent être pilotées pour atteindre les objectifs (temps, compétences, énergie, matériel, finance, informations) par des outils spécifiques relatifs à la gestion du temps, des compétences, à la veille informationnelle, à la planification des actions…

➢ La gestion de la sécurité nécessite de piloter l'atteinte des objectifs de sécurité et de conformité de l'organisation.

D/ L'atteinte des objectifs nécessitent la canalisation des comportements

Chacun poursuit ses objectifs qui peuvent être différents des objectifs imposés. On voit donc apparaitre des stratégies individuelles de comportements tantôts convergentes, tantôts divergentes.

L'organisation vit avec cette multiplicité qui contrarie ou favorise l'atteinte de ses objectifs.

Le management doit donc canaliser les comportements vers la stratégie de l'entreprise.

- La gestion de la sécurité nécessite un engagement du management qui oriente les comportements vers la réalisation des objectifs.

E/ Conclusion

La gestion de la sécurité et de la conformité devrait être intégrée au cœur du fonctionnement de l'entreprise :

- En étant présente dans la stratégie globale de l'entreprise (arbitrage) avec la définition et l'atteinte d'objectifs (performance de sécurité) ;
- En bénéficiant de ressources ;
- En bénéficiant d'une structuration ;
- En canalisant les comportements vers la stratégie de sécurité.

Si la gestion de la sécurité et de la conformité n'est pas intégrée dans la gestion globale de l'organisation elle sera peu efficace.

4.2. Les dysfonctionnements et la maîtrise des risques

Comment expliquer les dysfonctionnements et la diminution de la maîtrise des risques qu'ils engendrent ?

Le fonctionnement des organisations est influencé deux types de facteurs systémiques **en interaction :**

- Les facteurs **structuraux**, stables, comme les installations, les équipements, les processus, l'organigramme, les mentalités dans l'entreprise (etc.) qui conditionnent les comportements.
- Les facteurs **comportementaux**, volatiles, comme les caractéristiques de chaque individu, l'appartenance à un certain service, l'appartenance à une catégorie professionnelle (etc.) qui réagissent en conséquence.

Cela revient à considérer toute unité de travail comme un ensemble de **structures en interaction avec des comportements humains**. Cette interaction peut générer un fonctionnement recherché et attendu ou au contraire **des dysfonctionnements qui impactent la sécurité.**

Exemple : La mise en place d'un processus (structure) interagira avec des individus (comportement) de façon positive ou négative. Dans ce dernier cas, il n'est pas sûr qu'il soit effectivement respecté.

Ce constat amène une conséquence pratique : si l'on veut agir sur les dysfonctionnements et le niveau de maîtrise des risques de l'organisation, il est nécessaire de conduire des actions à la fois sur les structures et sur les comportements.

Exemple :
Actions sur la structure : Le nouveau processus devra avoir été optimisé avant son introduction (travail collaboratif, détermination d'un réel besoin…)
Actions sur les comportements : Son introduction auprès des personnels devra être accompagnée par le management (explications, formation, temps passé…)

Concrètement, ces interactions se manifestent dans les domaines de fonctionnement suivants :

- **les conditions de travail** (Espace de travail, nuisances, Matériels et outils…)
  Exemple de dysfonctionnement associé : Tâches mal assumées par manque d'outillage ;
- **l'organisation du travail** (Structuration, répartition du travail…)
  Exemple de dysfonctionnement associé : Cloisonnement ;
- **la communication-coordination-concertation** (Tout type d'échange)
  Exemple de dysfonctionnement associé : Manque de transmission d'informations de sécurité ;
- **la gestion du temps** (Planification, répartition du temps entre différentes activités…)
  Exemple de dysfonctionnement associé : Fragmentation des tâches, dispersion ;
- **la formation** (Compétences disponibles, besoin de formation…)
  Exemple de dysfonctionnement associé : Pas d'apprentissage des événements de sécurité ;
- **la définition et la mise en œuvre de la stratégie** (formulation claire, déclinaison en actions concrètes…)
  Exemple de dysfonctionnement associé : Les objectifs de sécurité sont peu définis / insuffisamment mis en œuvre.

Ces six domaines constituent une grille de référencement utile à la fois pour identifier les dysfonctionnements et pour rechercher des leviers d'amélioration.

Exemple :
Des procédures de gestion du maintien de la navigabilité ne sont pas suffisamment respectées (dépassement de butées d'entretien).
A quoi ces manquements sont-ils associés ? Formation insuffisante ? Manque de coopération avec la maintenance ? Conditions de travail inadaptées ? Manque de respect des règles du jeu ?

Les actions d'amélioration seront en correspondance avec les domaines de dysfonctionnements identifiés : actions sur la formation, l'amélioration de la coopération, les conditions de travail, l'encadrement des comportements…

Attention ! Une non-intervention sur les dysfonctionnements conduit à leur aggravation.

4.3. Management et pilotage

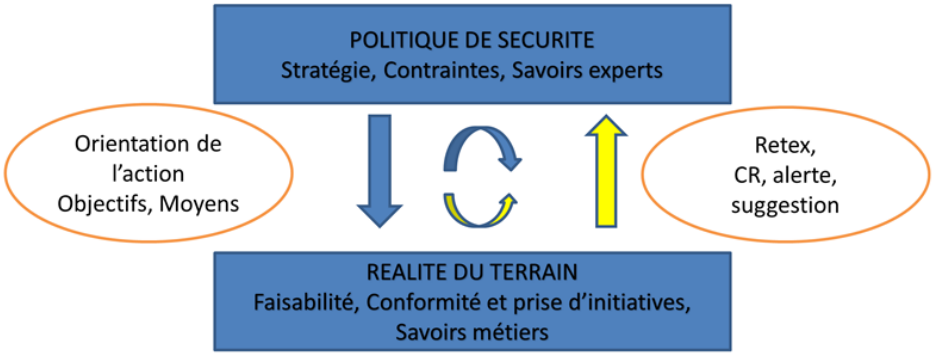
L'ensemble de la chaîne managériale joue un rôle clé dans la sécurité par le leadership qu'elle exerce.

Direction (DR) et Management (RDE) assurent le leadership en matière de sécurité. Les opérateurs s'impliquent au niveau de la gestion de la sécurité et de l'application des règles de sécurité

Direction, management et opérateurs ont des fonctions, des connaissances différentes mais complémentaires qui réunies permettent :

- Un maintien de la vigilance (on ne maîtrise vraiment jamais tout) :
  La remontée et l'analyse d'événements, la résolution des problèmes.
- Une logique de progrès continu :
  Les procédures sont perfectibles. Nécessité d'une participation collective à l'élaboration des règles.
- Un renforcement de la présence managériale sur le terrain :
  Observer, écouter informer, remonter, stimuler la vigilance aux risques.

Les pilotages complémentaires



Le Responsable est au cœur de l'articulation entre la direction et les opérateurs (spécificité du terrain). Il doit être exemplaire en matière de sécurité.

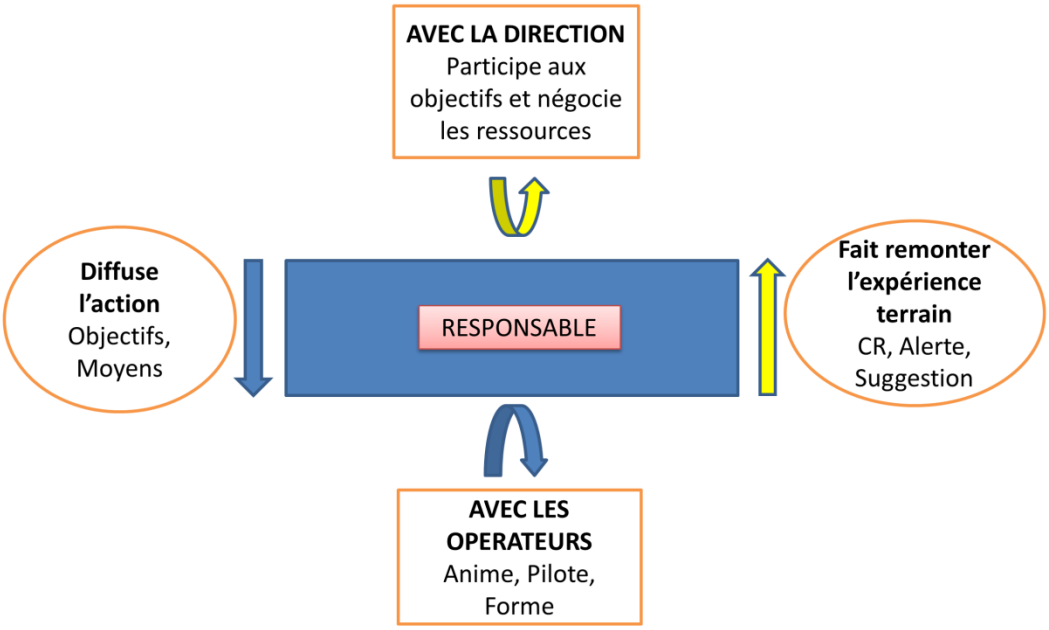
Positionnement par rapport à la direction :

- Il participe à la définition des objectifs ;
- Il négocie les moyens nécessaires à la sécurité ;
- Il organise et pilote l'application des décisions.

Positionnement par rapport au personnel opérateur :

- Il favorise le retour d'expérience sur la sécurité au quotidien et lors d'incidents ;
- Il associe les opérateurs à la formalisation des procédures les concernant et à la gestion du changement ;
- Il exprime le besoin de formation des opérateurs.

Le leadership sécurité du Responsable Désigné



4.4. Notions sur le concept de Facteurs Organisationnels et Humains (FOH)

La sécurité est assurée par le travail quotidien des différents métiers.
Lors d'un accident, c'est très souvent l'erreur humaine qui est désignée coupable. Or l'erreur humaine n'est pas **l'ultime cause** mais **la conséquence d'autres défauts** qui n'apparaissent que si l'on s'intéresse aux facteurs organisationnels et humains de la sécurité.

On compte quatre composantes dans les facteurs organisationnels et humains qui contribuent à la sécurité :

- **les individus :** compétences, formation, état de santé…
- **la situation de travail :** conçue ou non en fonction des propriétés humaines et des tâches à réaliser,
- **les collectifs de travail :** qualité des collectifs et des débats, transmission, vigilance partagée…
- **l'organisation et le management :** notamment le rôle des managers, l'implication des salariés dans la mise au point des règles, le traitement participatif des situations problématiques…

Cette approche **permet d'identifier et de mettre en place les conditions qui favorisent des comportements plus sûrs** à tous les niveaux de l'entreprise.

Le comportement positif en matière de sécurité est à la fois conforme et adaptatif.

La gestion de la sécurité ne se limite pas à l'application des procédures : la situation n'est pas toujours celle qui avait été prévue. Il est nécessaire de s'en remettre également au professionnalisme des spécialistes métier.
Ainsi apparait la nécessité de gérer deux types de sécurité :

- **La sécurité réglée :** anticiper ce qui peut se passer, mettre en place des procédures et des barrières, avoir un comportement de conformité ;
- **La sécurité gérée :** capacité à adopter les bonnes réactions, avoir un comportement professionnel.

Interactions entre les deux :

- Les adaptations se font à l'intérieur d'un cadre de règles.
- Les situations nouvelles permettent de tirer des enseignements pour l'organisation.

4.5. La culture de sécurité

La culture de l'organisation comporte une partie relative à la sécurité de l'activité : *dans notre activité, avec nos valeurs, nos habitudes, quel poids à la sécurité dans nos arbitrages ? La priorité sera-telle donnée à la sécurité, au délai, au maintien de l'exploitation… ?*

La culture de sécurité peut être vue comme un ensemble de **manières de faire** et de **manières de penser** largement **partagées** par les acteurs d'une organisation à propos de la maîtrise des risques liés à ses activités.

Exemple : D'après Hollnagel, la culture de sécurité, dans une organisation, c'est « ce que font les gens lorsque personne ne les regarde ».

La culture juste :

La « culture juste », est *« une culture dans laquelle les agents de première ligne ou d'autres personnes ne sont pas punis pour leurs actions, omissions ou décisions lorsqu'elles sont proportionnées à leur expérience et à leur formation, mais dans laquelle les négligences graves, les manquements délibérés et les dégradations ne sont pas tolérés ».* Il s'agit de la définition donnée dans le règlement européen (UE) n°376/2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile.

L'aéronautique est une activité à risques qui met en œuvre des systèmes complexes où la sécurité est un facteur déterminant. Afin de faire progresser cette sécurité, la transparence et le partage des informations sont essentiels.

En instaurant un environnement fondé sur la confiance, la culture juste vise notamment à créer des conditions favorables à la notification des événements et donc à contribuer à une gestion efficace de la sécurité aérienne.

Direction générale de l'Aviation civile
Direction de la Sécurité de l'Aviation civile
50, rue Henry Farman
75720 PARIS CEDEX 15
Tél. : +33 (0)1 58 09 43 21
www.ecologie.gouv.fr