La Lettre de l'UNSA-IESSA
Ingénieurs Electroniciens des Systèmes de la Sécurité Aérienne
« Libres, ensemble »
Information locale CESNAC – 17 mai 2016

GT SÉCURITÉ : UN NOUVEAU « GUIDE MISO » …

Le prochain GT **Sécurité** aura lieu le 18 mai où sera présentée la **version 3.4** du « Guide MISO ». Elle sera applicable au 1er novembre. Nul doute que cette nouvelle version fera date : elle va en effet **exclure toute une catégorie de maintenance (même programmée) de l'obligation de MISO** ! Et ce, en contradiction avec la réglementation et notre SMS. De plus, elle va étendre la conduite des systèmes NA (actuellement limitée aux tests d'équipements redondants, à leurs basculements et aux mesures sur ceux-ci) à des **tests d'équipements NA non redondants**, ainsi qu'à d'**autres actions non limitées à la conduite** (c'est-à-dire allant au-delà du domaine SMC de notre licence ATSEP) !

Des notions oubliées, des rappels nécessaires

Ingénieur électronicien des systèmes de la sécurité aérienne

Les IESSA exercent un métier fondamental en tant qu'ils contribuent à la sécurité[1] des usagers et à la fluidité du trafic aérien en garantissant aux contrôleurs aériens et aux pilotes un ensemble de services aéronautiques intègres, disponibles et fiables (cf. devenir-iessa.fr).

> « Les ingénieurs électroniciens des systèmes de la sécurité aérienne sont chargés, dans les organismes de la navigation aérienne, d'assurer la maintenance et la supervision technique[2] des équipements et des systèmes qui contribuent à la sécurité des vols, de participer au développement de ces équipements et systèmes et d'exécuter, dans l'administration de l'aviation civile, des missions d'encadrement, d'instruction, d'étude ou de direction de service ou de partie de service. » (loi n° 90-557 du 2 juillet 1990 relative au corps des IESSA)

Le volet « opérationnel » de ce métier comprend la **conduite en temps réel[3] des systèmes de la sécurité aérienne**, leur **maintenance**, la coordination avec les contrôleurs aériens et les prestataires et le maintien des services navigation aérienne (cf. plaquette IESSA / ENAC).

1 « la sécurité aérienne dépend principalement du contrôle assuré par les ingénieurs du contrôle de la navigation aérienne » (Conseil d'État, Assemblée, 4 avril 2014, n° 362785, 362787, 362806, 362811, 362813, 362815, …)

2 La ***surveillance*** (supervision passive) et le ***contrôle-commande*** (arrêt, relance, basculement, …) constituent les deux activés de la **fonction « supervision »** ou SMC (cf. cours de supervision, arrêté du 29 janvier 2016, etc.).

3 La conduite est toujours, et nécessairement, en temps réel et cette redondance informationnelle le rappelle utilement.

Conduite des systèmes de la navigation aérienne

Le Larousse définit la **conduite** (en cybernétique) par l'« action humaine ou automatique visant à ***gouverner l'évolution d'un système*** en modifiant son état par l'intermédiaire d'organes appropriés et en s'assurant que son comportement est bien celui que l'on désire »[4].

Le **conducteur de systèmes industriels**[5] intervient sur des installations automatisées ou non, de transformation, d'élaboration et de conditionnement par procédé continu, discontinu ou mixte. Il est chargé d'assurer la ***production*** industrielle sur un système automatisé ou non. Les tâches dans la conduite d'un système industriel[6] sont notamment de :

- ✔ **s'assurer des conditions de sécurité** ;
- ✔ identifier et prendre connaissance des prescriptions de réalisation, des consignes ;
- ✔ remédier ou alerter en cas de non-conformité du produit ou du process ;
- ✔ renseigner les documents de lancement de production ou de prise de poste ;
- ✔ mettre en marche la machine, le système, l'installation ;
- ✔ produire, contrôler et ajuster les paramètres relatifs au produit, au procédé, à l'installation ;
- ✔ **réagir en cas de dérive anormale, d'aléas ou de situation à risques** ;
- ✔ **appliquer les procédures de marche en mode dégradé** ;
- ✔ transmettre les consignes ;
- ✔ participer à la résolution de problèmes ;
- ✔ **réaliser une opération de maintenance de premier niveau** ;
- ✔ contribuer au diagnostic et aux opérations de maintenance préventive et corrective.

Quelques exemples de conduite de systèmes dans divers secteurs d'activité :

- conduite d'équipement de production chimique ou pharmaceutique ;
- conduite d'installation automatisée de production électrique, électronique, … ;
- conduite d'installation automatisée ou robotisée de fabrication mécanique ;
- conduite, surveillance de machines (supervision des installations industrielles) ;
- conduite de processus/procédés (module « supervision » dans la formation GEII)[7] ;
- conduite en temps réel des systèmes de la sécurité aérienne (IESSA).

À la direction des opérations, une intervention est dite de « **conduite technique de systèmes** » si[8] :

1. elle est explicitement répertoriée en tant que telle dans le **manuel ST**[9] (et a donc fait préalablement l'objet d'une réflexion sécurité[10]) et
2. les opérations se font via un panneau de commande (ou IHM) ou via des prises spécifiquement prévues à cet effet et sont limitées à des **tests d'équipements redondants**, des **mesures** ou des **basculements** (toutes ces opérations ayant été explicitement identifiées comme sans risques particuliers) et
3. elle est exécutée usuellement par du **personnel habilité**.

Du moins, jusqu'à présent…

4 Le synonyme de conduite est d'ailleurs « pilotage ».
5 Les certifications actuelles sont « conducteur de systèmes de production automatisée », « conducteur d'équipements industriels », « conducteur de procédé de fabrication », etc.
6 Cf. Certificat d'Aptitude Professionnelle « Conduite de systèmes industriels »
7 Cf. Diplôme Universitaire de Technologie « Génie Électrique et Informatique Industrielle »
8 Cf. Méthodologie d'Intervention sur Systèmes Opérationnels (MISO) actuellement en vigueur.
9 À l'évidence, il s'agit du « manuel d'exploitation des services techniques » (cf. manuel de management DSNA).
10 Cette « réflexion sécurité » est bien une étude de sécurité : la réglementation du ciel unique européen l'impose.

SMC : « *system monitoring and control* »

Il y a trois documents de référence relatifs à la formation des ATSEP et, en particulier, des IESSA[11] :

- OACI : document 7192 « **Manuel de formation / Partie E-2 / Électroniciens en sécurité de la circulation aérienne (ATSEP)** » (ISBN : 978-92-9231-935-9)
- Eurocontrol : « **Specification for Air Traffic Safety Electronics Personnel Common Core Content Initial Training** » (ISBN : 978-2−87497-041-2)
- Eurocontrol : « **Guidelines for the Competence Assessment of Air Traffic Safety Electronics Personnel** »

Rappelons comment ils décrivent la fonction « *system monitoring and control* » ou SMC :

Manuel de formation / E-2 / Électroniciens en sécurité de la circulation aérienne (ATSEP) :

SMC : Surveillance du système et contrôle d'ordinateur

Surveillance et contrôle des systèmes

Les étudiants doivent pouvoir […] Expliquer les principes et les fonctions de la **surveillance** et du **contrôle à distance** de système : Poste SMC, matériel contrôlé, procédures techniques et opérationnelles de surveillance et de contrôle de système.

Specification for ATSEP Common Core Content Initial Training :

Five specialised domains have been identified. They are Communication, Navigation, Surveillance, Data Processing and **System Monitoring & Control (SMC)**.

SMC operators perform level A tasks. If level B tasks are required, these are performed under supervision or are delegated to appropriately qualified staff

Level A tasks: Level A maintenance tasks are primarily associated with immediate service restoration or reconfiguration ("front-panel level"). They are appropriate for staff that has been trained to understand the elements of equipment or system, their interrelationships and functional purpose, but does not require an in-depth knowledge of these elements.

Level B tasks: Level B maintenance tasks involve in-depth fault analysis at the system/equipment level ("functional level"). They are usually carried out by staff that has been trained for the more complicated maintenance tasks on the equipment/system.

Level C tasks: Level C maintenance tasks involve the detailed diagnosis of a software problem, of a faulty Line Replacement Unit (LRU), Printed Circuit Board (PCB) or module ("component level"). They usually require the use of automated test equipment at a suitable location and are usually carried out by staff that has been trained in detailed fault diagnosis and repair techniques.

Guidelines for the Competence Assessment of ATSEP :

9.2 System Monitoring and Control Training and Competence Assessment – Training Process

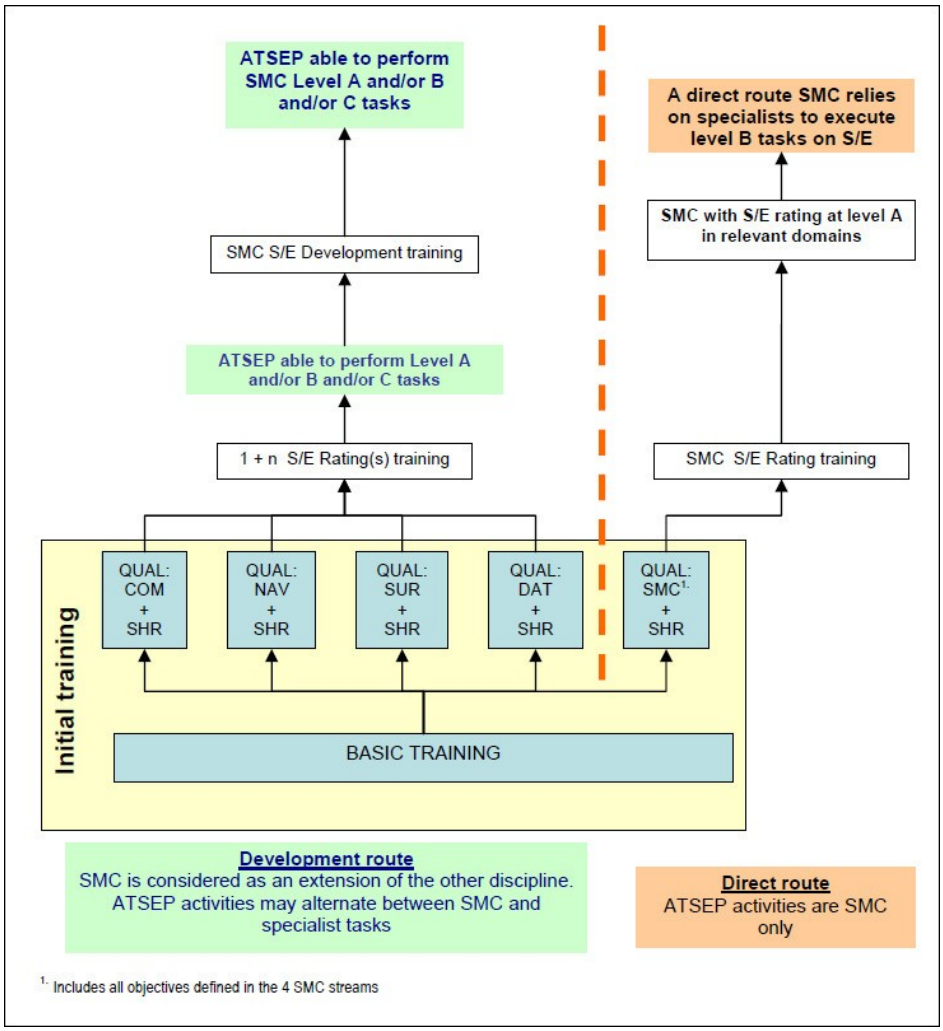
SMC ATSEP are normally sited at Area Control Centres and work at SMC suites or positions. They monitor the day to day operation of all operational systems/equipment in their area of responsibility. **The SMC ATSEP ensures that a quick response is made to malfunctions or failures by diagnosing the problem, activating fallback procedures and initiating the process of repair.** It may also be necessary for the **SMC ATSEP** to coordinate with adjacent Flight Information Region (FIR) personnel.

11 Ces documents sont à la base de notre cursus de formation (arrêté du 16 décembre 2014, …) et de la licence ATSEP.

Les qualifications de domaine ***Communication***, ***Navigation*** et ***Surveillance*** sont obligatoires pour maintenir des systèmes techniques délivrant les services CNS. La qualification ***Data Processing*** est obligatoire pour maintenir des systèmes techniques[12] délivrant les services ATS. Ces qualifications permettent également de superviser les systèmes des domaines correspondants.

La qualification de domaine ***System Monitoring & Control*** suffit pour superviser des systèmes contribuant à délivrer des services ATS ou CNS : mais en aucun cas pour les maintenir[13]. Ce domaine consiste à savoir poser un diagnostic d'un problème, à appliquer les procédures de secours et à être à l'initiative du processus de réparation. Il ne fait guère de doute qu'on parle bien là de la conduite technique de systèmes appliquée au contexte d'un prestataire de services ATS et/ou CNS.

On pourra noter qu'un opérateur SMC est normalement limité aux interventions de niveau A tel que définis par Eurocontrol[14]. Les interventions d'un niveau plus élevé relevant des spécialistes[15].



12 Notamment les systèmes de traitement des données de vol, les systèmes de traitement des données de surveillance et les systèmes d'interface homme-machine des contrôleurs aériens.

13 Actuellement, notre licence ATSEP impose de détenir, d'une part, au moins une qualification de domaine parmi communication, navigation, surveillance et traitement de données et, d'autre part, la qualification SMC.

14 Explanatory Material on ESARR 5 Requirements for Engineers and Technical Personnel Undertaking Operational Safety-Related Tasks (EAM 5 / GUI 3)

15 Un spécialiste de maintenance détient au moins une qualification de domaine parmi communication, navigation, surveillance et traitement de données.

Rôle du « superviseur technique multiqualifié » (STM)

La fonction de superviseur technique multiqualifié (STM) chargé de la maintenance opérationnelle a été créée à l'occasion de la réorganisation de la supervision technique du CESNAC dans le cadre du protocole DGAC de 2007 afin d'augmenter la polyvalence des agents de supervision technique[16]. Cette organisation s'appuie sur la mise en œuvre de la supervision technique centralisée (STC)[17]. Les différentes STS propres à chaque systèmes devant être reléguées en maintenance spécialisée.

GT Europe de la Navigation Aérienne et protocole d'accord social DGAC 2010-2012 :

Stratégie « technique » de la DSNA / La supervision

Pour la **maintenance opérationnelle**, l'objectif est de mettre en service une Supervision Technique Centralisée dans tous les centres opérationnels importants. Ce système standard sera interfacé avec les différentes chaînes et offrira des services et une IHM homogènes. Pour la **maintenance spécialisée** on cherchera à utiliser le plus possible les outils de maintenance fournis par l'industrie avec chacun des systèmes, tout en respectant quelques principes commun d'IHM (spécifications « STS light »).

Le STM assure la fonction SMC de la licence ATSEP consistant en la surveillance d'exploitation des systèmes techniques ATS et CNS ainsi que la permutation d'équipements redondants à partir d'un panneau de commande (ou IHM) ou via des prises spécifiquement prévues à cet effet. Ces opérations sont décrites dans le manuel d'exploitation mis à sa disposition et ont fait l'objet d'une étude de sécurité conformément aux exigences de sécurité du ciel unique européen. Il effectue ainsi les actions immédiates pour rétablir la meilleure disponibilité possible des systèmes CNS et ATS au service des pilotes et des contrôleurs aériens[18].

Par ailleurs, dans le cas où ces actions seraient également prévues dans son manuel d'exploitation et s'il dispose encore d'une STS, le STM peut surveiller l'état du bien et les paramètres significatifs de cet état, effectuer des actions prédéfinies de maintenance sur des éléments facilement accessibles en toute sécurité (en suivant les instructions de son manuel d'exploitation), voire même rétablir provisoirement une fonction requise par des opérations simples de dépannage (niveau 1). Ces actions relèvent de l'auto-maintenance, une maintenance accessible au personnel d'exploitation.

Manuel de traitement des événements Sécurité par les Services Techniques :

L'ensemble des **événements** est enregistré dans le journal de bord de supervision technique, dans le cadre de la maintenance opérationnelle.

Le SMI de la DSNA définit un « événement » comme un accident, incident ou tout autre défaut ou dysfonctionnement d'un aéronef ou d'un système fonctionnel de la DSNA ayant pour conséquence de « **compromettre le niveau de sécurité ou de sûreté** ». Pourtant, chacun constate que les PV du journal de bord font également état des non-conformités[19] : celles-ci représentent 99 % du contenu du journal. C'est ce que d'aucuns peuvent appeler des « signaux faibles »[20].

16 « L'évolution des techniques et des métiers doit permettre d'aller vers une plus grande polyvalence des agents de supervision technique. » (protocole d'accord social DGAC 2007-2009)

17 « Cette organisation s'appuiera notamment sur la mise en œuvre de la supervision technique centralisée (STC). » (protocole d'accord social DGAC 2007-2009), « Elle est nécessaire à la mise en œuvre de la réorganisation des supervisions opérationnelles » (BACEA 2011, 2012, 2013 et 2014)

18 Cf. manuel de traitement des événements Sécurité par les Services Techniques

19 « Écart ou Non-conformité : Non-satisfaction d'une exigence (exigence stipulée dans le règlement applicable ou dans le référentiel local) » (cf. « procédure de traitement des constats et des ACAP » - PRO_003/DSNA)

20 La pertinence d'une telle collecte est un vrai débat. Elle peut aussi induire une sur-réaction inappropriée lorsque les agents n'ont pas la culture sécurité : autrement dit, la maîtrise des exigences de sécurité.

Programme Fonctionnel Détaillé / Dialogue compétitif RENAR/ISOCRATE n° 04S0083 :

Référence : 8CR0402 / V2R0 du 15 février 2005

Dans la Navigation Aérienne, il y a deux types de maintenance, associés à des profils d'exploitant différents :

- **Maintenance opérationnelle :** il s'agit d'une **maintenance H24** réalisée par des exploitants locaux ayant des **compétences techniques très générales** sur RENAR Leur rôle est d'appliquer des **procédures simples** lorsque la situation l'exige, pour rétablir le service minimum nécessaire.
- **Maintenance spécialisée :** il s'agit d'une **maintenance à heure de bureau** et jour ouvrable réalisée par des exploitants locaux spécialistes de RENAR.

Protocole d'accord social DGAC 2007-2009 :

2-1.8. Evolution de la supervision technique et de la maintenance

L'évolution des techniques et des métiers doit permettre d'aller vers une plus grande polyvalence des agents de supervision technique. […]

Par ailleurs, tout en gardant le principe de l'alternance longue, sera étudiée au sein d'un groupe de travail issu de ce protocole, la possibilité d'aller vers une organisation de type 2+1 dans les CRNA et à Orly, 3+1 à CDG, 1+1 au CESNAC, avec un chef de supervision assurant une coordination renforcée avec le chef de salle, et des **superviseurs techniques multi qualifiés chargés de la maintenance opérationnelle**. Cette organisation s'appuiera notamment sur la mise en œuvre de la supervision technique centralisée (STC). Les superviseurs techniques multi qualifiés recevront une formation leur permettant d'élargir leur domaine de compétence et d'assurer la supervision de systèmes ou chaînes dépendant de différentes subdivisions.

Datalink Initial Operating Capability – Tranche 1 Bis / Déploiement CESNAC et 3 CRNA :

Référence : DTI/DSO/1512498/IVD / V1R0 du 18 novembre 2015

MO	**Maintenance Opérationnelle : Supervision H24** afin d'assurer la disponibilité opérationnelle. Le rôle utilisateur MO a pour mission la détection des pannes et le rétablissement du service (par relance, basculement, réaffectation) en s'aidant des fiches de maintenance. **La MO n'effectue pas de réparation**. Cf. MS.
MS	**Maintenance Spécialisée :** Le rôle utilisateur de Maintenance Spécialisée (ou MS, ou Spécialiste Produit) a pour mission la rédaction des fiches de maintenance pour la MO, l'établissement des diagnostics, la réparation des pannes, la maintenance préventive…

Wikipédia / Ingénieur Électronicien des Systèmes de la Sécurité Aérienne :

La conduite de systèmes en temps réel

Les IESSA sont amenés à assurer de la **maintenance opérationnelle** sur les systèmes techniques nécessaires au contrôle aérien. Pour cela, **les IESSA exploitent des systèmes de supervision qui permettent de détecter les dysfonctionnements et effectuent des tâches de dépannage en temps réel**, tout en assurant un niveau maximal de sécurité. Les IESSA sont spécialisés dans un grand domaine technique et interviennent spécifiquement dans leur domaine de compétence. Dans les grands centres de contrôle, comme les Centre En Route de la Navigation Aérienne (CRNA), **les IESSA assurant la conduite des systèmes**, dits "superviseurs", sont au nombre de 3 ou 4 en permanence, selon la configuration choisie localement. Ces centres fonctionnent 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

Dans le contexte européen, **les IESSA chargés de la conduite sont assimilés à des ATSEP**.

Disponibilité opérationnelle

La norme AFNOR NF EN 13306 « Terminologie de la maintenance » définit ainsi la disponibilité : « Aptitude d'un bien à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou durant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires est assurée ». Attention : il s'agit de la « **disponibilité intrinsèque** » (Di) du bien, car elle caractérise les qualités intrinsèques de celui-ci : l'absence des moyens de maintenance, d'alimentation en énergie, etc. ne sont pas pris en compte. C'est la disponibilité du bien du point de vue du fabriquant qui s'exprime par la formule « MTBF / (MTBF + MTTR) » et qui dépend de la fiabilité prévisionnelle du bien (MTBF[21]) et de sa maintenabilité intrinsèque (1 / MTTR[22]).

Dans la réalité de l'exploitation, des aléas de production[23], de maintenance[24] ou d'environnement[25] se produisent dégradant ainsi la « disponibilité intrinsèque ». La « **disponibilité opérationnelle** » (Do) est la disponibilité sur le terrain, vue de l'utilisateur ou du client. Cet indicateur d'exploitation se mesure[26] par la division du « **temps effectif de disponibilité** »[27] (somme des durées des « états de fonctionnement »[28] et des « états d'attente »[29]) par le « **temps requis** »[30]. Il faut souligner que le « temps effectif de disponibilité » peut intégrer des opérations de maintenance s'ils n'entraînent pas d'indisponibilité du bien, ce qui est notamment possible lorsque celui-ci intègre une redondance.

Décomposition des temps suivant AFNOR :

<table>
<tr><td colspan="8">TEMPS TOTAL</td></tr>
<tr><td colspan="7">TEMPS D'OUVERTURE</td><td rowspan="6">FERMETURE</td></tr>
<tr><td colspan="5">TEMPS REQUIS</td><td colspan="2">TEMPS NON REQUIS</td></tr>
<tr><td colspan="3">TEMPS DE DISPONIBILITÉ</td><td colspan="3">TEMPS D'INDISPONIBILITÉ</td><td rowspan="3">TEMPS POTENTIEL DE DISPONIBILITÉ + RÉNOVATIONS IMPORTANTES</td></tr>
<tr><td colspan="2">TEMPS DE FONCTIONNEMENT</td><td rowspan="2">TEMPS D'ATTENTE (STANDBY)</td><td rowspan="2">TEMPS D'INCAPACITÉ POUR CAUSES EXTÉRIEURES</td><td rowspan="2">APRÈS DÉFAILLANCE (OU AVANT REMISE EN SERVICE)</td><td rowspan="2">POUR MAINTENANCE PRÉVENTIVE</td><td rowspan="2">POUR CONTRAINTES D'EXPLOITATION[31]</td></tr>
<tr><td>TEMPS UTILE</td><td>NON QUALITÉ</td></tr>
<tr><td colspan="3">TEMPS EFFECTIF DE DISPONIBILITÉ</td><td colspan="4">TEMPS D'INCAPACITÉ</td></tr>
</table>

La norme NF E60-182 donne une formule légèrement différente : « temps de fonctionnement »[32] divisé par le « temps requis » (Tf / Tr). Toutefois, elle intègre les temps d'attente (« *stand-by* ») dans sa définition du temps de fonctionnement (ou, plus exactement, ne les considère pas).

21 MTBF : « *Mean Time Between Failures* » (temps moyen de bon fonctionnement entre défaillances)
22 MTTR : « *Mean Time To Recovery/Repair/Replace/Restore/...* » (temps moyen jusqu'à la remise en service)
23 Défaut de matières premières, casse d'outillage, erreurs humaines, autres incident de production, …
24 Manque de pièces de rechange, outillage défectueux, indisponibilité du personnel de maintenance, …
25 Panne de l'alimentation en énergie, causes climatiques, absentéisme, grève des personnels, …
26 Cf. AFNOR XP X60-020 (rem. : attention à bien distinguer la disponibilité opérationnelle prédite de celle mesurée)
27 « État effectif de disponibilité : État dans lequel l´entité est effectivement apte à accomplir une fonction requise et où la fourniture des moyens extérieurs éventuellement nécessaires est assurée » (AFNOR X60-500)
28 « État d'un bien qui accomplit une fonction requise » (NF EN 13306)
29 « État d'un bien qui est à fois disponible et en état de non-fonctionnement pendant le temps requis » (NF EN 13306)
30 « Durée pendant laquelle l'utilisateur demande que le bien soit en état d'accomplir une fonction requise » (N.13306)
31 Changement d'outil selon les programmes de fabrication, contrôle sur l'entité même du produit fabriqué, …
32 « Durée pendant laquelle un bien accomplit sa fonction requise » (NF EN 13306)

Redondance et secours

Une faute provoque une erreur (un comportement erroné) susceptible d'entraîner une défaillance[33]. La faute, cause de l'erreur, peut elle même s'avérer être la panne[34] d'une autre entité :

… → [défaillance (panne) | **FAUTE**] → **ERREUR** → < ? > → [**DÉFAILLANCE (PANNE)** | faute] …

La **défaillance** est la « cessation de l'aptitude d'un bien à accomplir une fonction requise » et la **redondance** est l'« existence dans un bien de plus d'un seul moyen à un instant donné pour accomplir une fonction requise » (NF EN 13306) : par suite, il n'y a pas de défaillance lorsque la fonction requise est rendue, et ce, même si un ou plusieurs moyens redondants, internes au bien et lui permettant d'accomplir la fonction requise sont en panne. Ce principe est à la base des systèmes tolérant aux pannes (ou aux fautes), que celles-ci soient d'origine matérielle, logicielle ou humaine. **La redondance permet d'éviter la défaillance sur une, voire même plusieurs pannes.**

De manière très synthétique :

- avec un système non redondé : panne du moyen → défaillance du bien
- avec un système redondé : panne du 1er moyen × panne du 2e moyen × … → défaillance du bien

Tous les moyens prévus pour accomplir la fonction requise doivent être en panne pour entraîner une défaillance. Après une défaillance, le bien est en panne, totale ou partielle[35]. La panne d'un moyen redondant n'aboutit donc pas à la panne, même partielle, du bien : la redondance devant justement permettre au bien de continuer à accomplir sa fonction, même avec un élément en panne[36].

La redondance peut concerner les moyens techniques (matériels, logiciels) ou humains (personnels). Elle permet ainsi de ne plus rendre tributaire la disponibilité d'un bien des temps de remise en état de fonctionnement ; pour ne tenir compte que, le cas échéant, des temps de reprise. Cette technique augmente la disponibilité du bien en multipliant les éléments (équipements, logiciels ou acteurs), mais au détriment de la simplicité entraînant une fiabilité réduite et un besoin d'entretien accru[37].

La redondance peut être **active**[38] (parfois appelée « partage de charge »). Ex : avion multi-moteurs, camions aux roues multiples, *multi-link trunking*, RAID 6, *cluster* de calcul, etc. Ou **passive**[39] (aussi appelée redondance séquentielle ou bascule « normal / secours » ou du type « *stand-by* »). Ex : roue de secours, parachute de secours, onduleur, RAID 1, secours ultime (image radar), etc.

On peut distingue trois types de secours (redondance passive) :

- secours "froid" : le secours est mis en œuvre (démarré, etc.) seulement lorsque l'équipement tombe en panne (le secours ne peut pas tomber en panne tant qu'il n'est pas mis en marche) ;
- secours "chaud" : tous les équipements fonctionnent en parallèle et sont associés à une politique de prise en main ou un mécanisme de détection/sélection ;
- secours "tiède" : le secours est "allumé" mais sans être en fonction/service.

33 Le traitement d'erreur vise à éliminer une erreur (due à une panne) avant qu'elle ne produise une défaillance.
34 « Une défaillance est un événement à distinguer d'une panne qui est un état. » (NF EN 13306)
35 Le bien ne peut plus remplir une partie de ses fonctions.
36 « La tolérance de panne est la propriété d'un calculateur de se reconfigurer automatiquement, lors d'une défaillance, sur l'élément matériel similaire disponible » (revue technique du STNA n° 37 / « L'AERMAC … »)
37 Un système redondé nécessite plus de moyens pour sa conception, pour son exploitation et pour sa maintenance.
38 « tous les moyens pour accomplir une fonction requise [sont] simultanément en fonctionnement » (NF EN 13306)
39 « une partie des moyens nécessaires pour accomplir une fonction requise est en fonctionnement, le reste de ces moyens n'étant utilisé qu'en cas de besoin » (NF EN 13306)

Basculement « normal / secours » à la DSNA

Les systèmes intégrant une bascule « normal / secours » sont très utilisés dans les systèmes à haute et très haute disponibilité, notamment dans les systèmes des services de la navigation aérienne :

> Toute variation hors tolérance des grandeurs contrôlées se traduit par une alarme qui déclenche automatiquement le **basculement** sur l'ensemble d'émission de **secours**, celui-ci étant en permanence sous tension.[40]
>
> Le SYStème de BASculement (SYSBAS) a pour fonction d'aider à assurer la **disponibilité maximum** des applications du serveur ATC. Il surveille donc les applications et, en fonction de critères déterministes, décide du **basculement Principal Secours**.[41]
>
> Mise en place au niveau de la chaîne radio d'un dispositif de **basculement** automatique sur détection de panne pour assurer le passage de la fréquence de la station **normale** vers la station **secours**.[42]

Le basculement prévu peut être automatique, mais également manuel :

> **Ce basculement est soit manuel** (deux panneaux de basculement le permettent, l'un local, l'autre déporté) soit automatique (seulement dans le sens S.P.N.).[43]
>
> En particulier, l'absence d'une maintenance permanente a conduit […] à intégrer **sur les positions de contrôle** le basculement d'une couverture normale sur une couverture de secours.[44]
>
> La **STC** présente une vision globale et cohérente de tous les moyens techniques d'un site. Dans les CRNA et au CESNAC, elle doit aussi permettre de rétablir rapidement l'intégrité de la fonctionnalité en cas de panne (par **basculements** et reconfigurations, en ne se souciant pas, dans un premier temps, du diagnostic de la panne).[45]

Lorsque le basculement est manuel, il fait ainsi partie de la conduite (technique) du système.

> **« Le CRNA/Est, vitrine du STNA et de l'industrie française / La supervision technique »[46] :**
>
> La position de supervision technique du CRNA/Est a été particulièrement étudiée pour fournir à **l'ingénieur de la sécurité aérienne, en charge de la supervision**, toutes les informations dont il a besoin pour assurer sa mission. Il dispose pour cela de tous les déports et alarmes des chaînes à surveiller (radar/visualisation, radio, téléphone, énergie, etc.) et des calculateurs CAUTRA. **Des platines de reconfiguration et de télécommande permettent de faire les basculements normal/secours**.

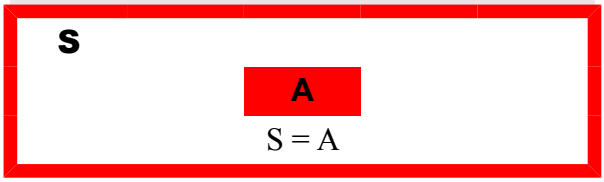
Assurer un basculement « normal / secours »[47] est une action d'exploitation. Rétablir la redondance en réparant l'élément en panne et en le réintégrant dans le système technique est une action de maintenance[48]. Une grande partie peut être réalisée alors même que le bien est en fonctionnement : c'est l'autre apport du principe de redondance. Mais le principal intérêt est, bien sûr, d'éviter la défaillance fonctionnelle du bien qui continue ainsi d'assurer toutes les fonctions requises[49].

---

40 Revue technique du STNA n° 3 / « Les systèmes d'atterrissage aux instruments standardisés (ILS) »
41 Revue technique du STNA n° 57 / « Cautra sous Unix »
42 Revue technique du STNA n° 64 / « Cohabitation Radar Monopulse - VHF »
43 Revue technique du STNA n° 31 : « La nouvelle chaîne radio des CRNA »
44 Revue technique du STNA n° 35 : « Traiter et distribuer les voies radiotéléphoniques »
45 Revue technique du STNA n° 66 : « L'harmonisation des supervisions techniques »
46 Le temps des ingénieurs de la navigation aérienne – Mémoires techniques – 1945-1985
47 Formellement on parle ici de redondance séquentielle ou, plus communément, de redondance passive.
48 De maintenance (corrective) curative pour être précis.
49 Au temps de détection de panne et de basculement près.

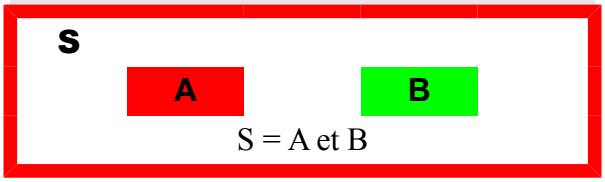
Rappel des différents types de redondance

Système S avec un unique équipement A (absence de redondance)



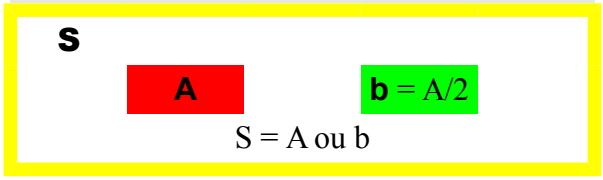
Défaillance (panne totale)
Le système est indisponible

Système S avec deux équipements A et B en série



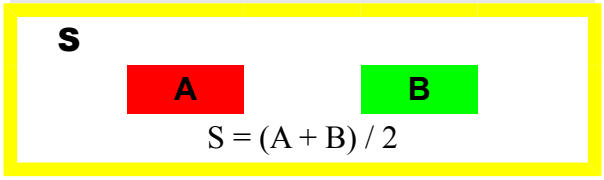
Défaillance (panne totale)
Le système est indisponible

Système S avec deux équipements A et B en redondance passive partielle



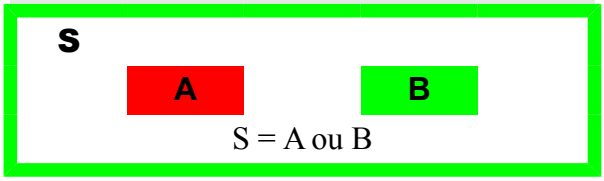
Défaillance (panne partielle)
Fonctionnement dégradé
Le système est disponible, mais dégradé

Système S avec deux équipements A et B en redondance active (partage de charge)



Défaillance (panne partielle)
Fonctionnement dégradé
Le système est disponible, mais dégradé

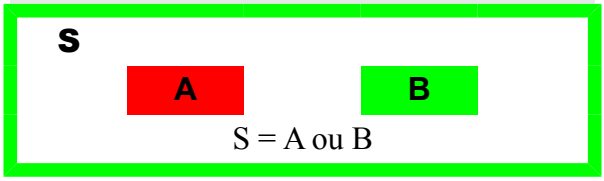
Système S avec deux équipements A et B en redondance passive (totale)



Aucune défaillance
Fonctionnement normal (nominal)
Le système est disponible
SYSTÈME TOLÉRANT AUX PANNES
La panne est transparente aux opérateurs. Les mainteneurs interviendront à l'occasion du prochain arrêt programmé.

Les architectures tolérantes aux fautes utilisent ce type de redondance qui augmente la sûreté de fonctionnement et en particulier la disponibilité.

Système S avec deux équipements A et B en redondance active totale



Aucune défaillance
Fonctionnement normal (nominal)
Le système est disponible
SYSTÈME TOLÉRANT AUX PANNES
La panne est transparente aux opérateurs. Les mainteneurs interviendront à l'occasion du prochain arrêt programmé.

La défaillance du système ne survient qu'après la panne du dernier composant survivant. Cette redondance est plus complexe et plus chère.

Revue technique du STNA n° 37 / « L'AERMAC » :

La tolérance de panne permet d'éviter ces écueils et propose fonctionnellement deux machines en ligne. **La défaillance est transparente à l'utilisateur ET AUX SUPERVISEURS** à ce point que le remplacement de carte se fait sous tension et en fonctionnement.

Danger inhérent aux opérations de maintenance, surtout palliative

La **maintenance** est définie par la norme NF EN 13306 « Terminologie de la maintenance » comme l'« Ensemble de toutes les actions techniques, administratives et de management durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise ». Elle est notoirement reconnue comme étant une activité dangereuse[50].

> **Externalisation de la maintenance et sécurité, une analyse bibliographique (D. Tazi) :**
>
> ***CSI (« Cahiers de la Sécurité Industrielle »), Institut pour une Culture de Sécurité Industrielle***
>
> « **les situations relatives aux opérations de maintenance, réalisées en interne ou externalisées doivent être considérées comme dangereuses par nature** »
>
> « la responsabilité pénale de la hiérarchie est engagée, pour tout accident de travail consécutif à une opération de maintenance ou à une défaillance d'un appareil soumis à règlement »
>
> « La maintenance contribue à la maîtrise des risques d'une installation en améliorant la fiabilité et la sécurité des équipements de production ; **les activités de maintenance sont toutefois dangereuses** et peuvent porter atteinte à la santé et la sécurité des employés. »
>
> « Concernant la maintenance dans les industries de procédés, les écrits sont souvent internes aux entreprises et se présentent sous forme de guides de bonnes pratiques […]. **Les guides soulignent la dangerosité des activités de maintenance et prônent une préparation et une supervision stricte de ces activités**. »

La **maintenance palliative**[51] est, avec la **maintenance curative**, une des deux subdivisions de la **maintenance corrective**. La norme AFNOR FD X60-000[52] la décrit ainsi :

> « Action de maintenance corrective destinée à permettre à un bien d'accomplir provisoirement tout ou partie d'une fonction requise. Appelée couramment « **dépannage** », la maintenance palliative est principalement constituée d'actions à caractère provisoire qui doivent être suivies d'actions curatives. »

Si la maintenance curative est une action ayant pour objet de rétablir un bien dans un état spécifié[53], qui peut être un état dégradé[54], pour lui permettre d'accomplir une fonction requise, la maintenance palliative est, comme rappelé ci-dessus, une action destinée à permettre à un bien d'accomplir provisoirement tout ou partie d'une fonction requise. Lorsque la pièce, l'outillage ou la compétence n'est pas disponible et si on considère que l'arrêt du bien n'est pas acceptable, on peut essayer de « se débrouiller »[55]. **La maintenance palliative est particulièrement dangereuse**, puisqu'elle n'emploie pas forcément un moyen prévu à cet effet et que, surtout, le bien une fois dépanné avec « les moyens du bord »[56] ne répond rigoureusement plus aux spécifications. On comprend dès lors pourquoi un dépannage ne peut que pallier provisoirement à la panne d'un bien, dans le sens que ce temps est incertain. Une action de dépannage[57] ne devrait être faite qu'en faisant la balance entre le danger que pourrait éventuellement représenter un arrêt prolongé du bien et celui inhérent à toute maintenance palliative : car, ne s'attaquant pas à ses causes, elle ne permet pas de se prémunir contre une répétition de la panne ou une aggravation de la situation qui peut alors devenir ingérable.

---

50 Cf. Maintenance : des activités à risques (INRS), Maintenance / Prévention des risques professionnels (INRS), etc.
51 Sa traduction en anglais est « ***stop-gap maintenance*** », soit littéralement « **maintenance bouche-trou** »…
52 Le fascicule de documentation FD X60-000 a été très récemment remplacé par la norme NF X60-000.
53 Cf. FD X60-000
54 Un ou plusieurs niveaux de fonctionnement dégradé peuvent (ou pas) avoir été prévus lors de la conception du bien.
55 Cf. « Maintenance : concepts et définitions » Editions Techniques de l'Ingénieur
56 Bernard MECHIN, animateur des GT Afnor X60-000, du WG4 européen (NF EN 13306) et ex-directeur du CIMI
57 À distinguer de la réparation qui est le propre de la maintenance curative.

Maintenance : la méthode Maxer / Pannes et dépannages (R. Sanner, S. Sanner)[58] :

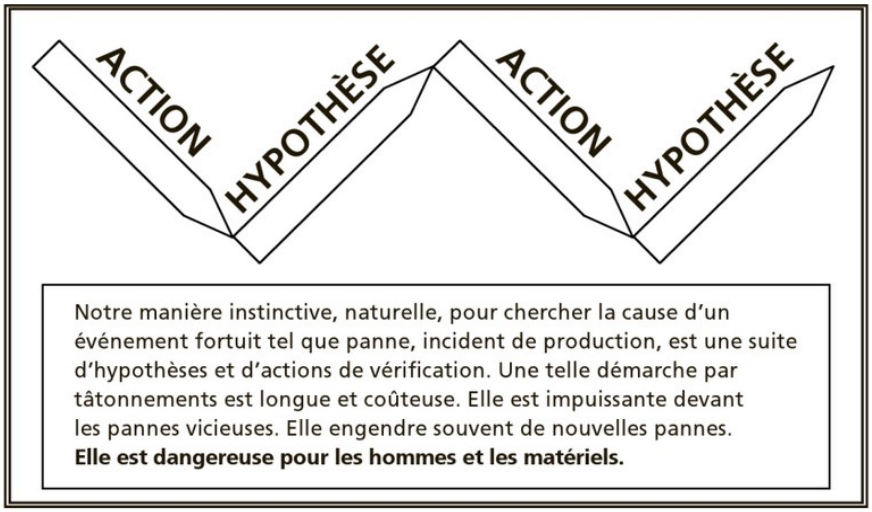


Figure 2.2 – Dépannage en dents de scie.

Maintenance palliative

« Elle est dangereuse pour les hommes et les matériels. »

« Mais souvent, on fait des hypothèses et leur vérification sans trouver la cause. Cette façon de faire prend du temps, coûte cher et risque d'introduire de nouvelle pannes dans le système. »

« On agit sur les effets sans corriger la cause. C'est le remède symptomatique des médecins. Une telle intervention peut être dangereuse, puisqu'elle masque la cause qui continue à agir. »

« le remède proposé est dangereux (il est palliatif) »

La nature palliative de ce type de maintenance peut être illustrée par les exemples suivants :

- une rustine pour obturer un trou d'une chambre à air afin d'essayer de terminer sa course[59] ;
- le bâchage d'une toiture suite à une avarie et en attendant la réparation définitive[60] ;
- un panneau de bois pour remplacer temporairement un vitrage cassé[61] ;
- la mise en place de papier aluminium autour d'un fusible fondu ou pire.

Toute maintenance palliative est un cas d'espèce, mais elle ne doit jamais être la première méthode choisie dans une politique de maintenance qui ne doit pas viser à assurer coûte que coûte la fonction du bien dans des conditions autres que celles de la sûreté de fonctionnement (sécurité, disponibilité, fiabilité et maintenabilité)[62]. Le palliatif est caractéristique du 2e niveau de maintenance proposé par la norme FD X60-000 et le curatif des 2e et 3e niveaux de maintenance de cette même norme[63].

Organisation de la maintenance et interactions maintenance-production ... (C. Grusenmeyer) :

INRS (« Institut National de Recherche et de Sécurité »), site web : www.inrs.fr

« Les opérateurs de production ne paraissent, en effet, pas toujours disposer des informations, des moyens ou des connaissances et compétences nécessaires à la réalisation de ces opérations. **La prise en charge d'opérations de dépannages par ces opérateurs peut ainsi donner lieu à des situations potentiellement dangereuses**. » (page 42)

« Ainsi, et sur la base des entretiens, les tâches de maintenance assurées par les opérateurs de production constituent non seulement des opérations de maintenance de premier niveau, mais aussi des opérations de dépannage, bien que celles-ci ne fassent pas partie de leurs attributions. **Ces difficultés d'identification de leurs tâches par les opérateurs peuvent par conséquent donner lieu à des situations potentiellement dangereuses, ces derniers ne disposant pas des compétences ou des moyens nécessaires à la réalisation de telles opérations.** » (page 82)

58 Collection « Technique et Ingénierie », Dunod / L'Usine Nouvelle
59 Remarque : une roue de secours, même compacte, est une redondance (du type « normal/secours ») prévue.
60 Exemple tiré de l'ouvrage *La maintenance du patrimoine bâti - Optimiser la gestion technique des bâtiments publics* rédigé par un collège d'experts et de juristes.
61 Exemple cité par le site professionnel QUADRA-TECH.
62 Des circonstances particulièrement graves et urgentes peuvent nécessiter le recours à une maintenance palliative.
63 Cf. FD X60-000, support de cours en ligne BTS MI sur la maintenance corrective

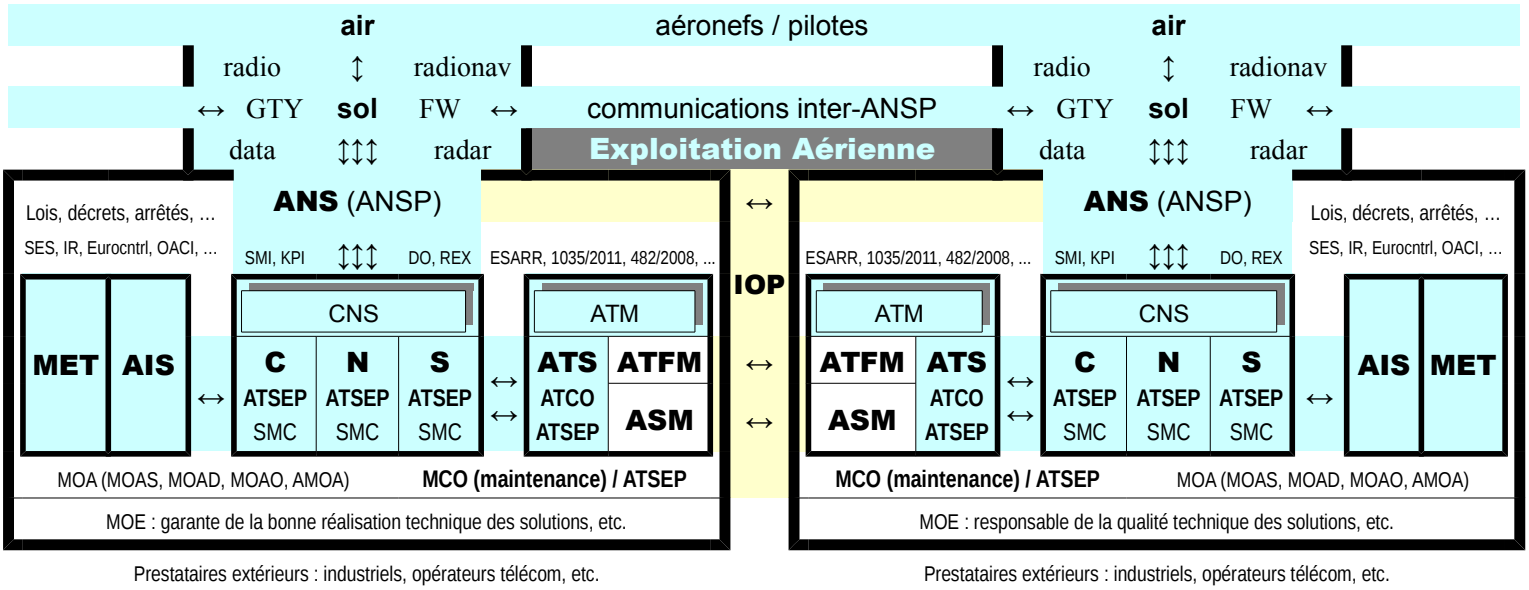
Exploitation et maintenance (et les personnels afférents)

La littérature[64] distingue le **personnel d'exploitation** du **personnel de maintenance** : ces domaines étant exclusifs l'un de l'autre. Cette distinction est importante lors de l'analyse de certains modes de défaillance et, en particulier, dans le cadre de la redondance. Ce qui ne signifie pas que le personnel d'exploitation ne peut pas accéder à certaines ***actions de maintenance*** et réciproquement.

Le **personnel d'exploitation** comprend[65] le **personnel de conduite**, le **personnel de production** et l'**utilisateur**. Le **personnel de conduite** assure la veille du bien (surveillance en fonctionnement). Afin de mieux situer ces notions, voici une application dans les services de la navigation aérienne :

<table>
<tr><td colspan="3">personnel d'
Exploitation
Manuel d'exploitation</td><td>personnel de
Maintenance
Instructions de maintenance</td></tr>
<tr><td>client / utilisateur (final)
Utilisation
Manuel d'utilisation</td><td>personnel de
Production
Manuel de production</td><td>personnel de
Conduite (technique)
Manuel de conduite</td><td>personnel de
Maintenance
Instructions de maintenance</td></tr>
<tr><td>pilotes d'aéronefs
Trafic aérien (vols)
MANEX</td><td>contrôleurs aériens
Contrôle aérien
MANEX</td><td>superviseurs techniques
Supervision technique
MANEX</td><td>spécialistes
Maintenance spécialisée
Volet « procédure » d'une MISO</td></tr>
</table>

Les manuels d'exploitation (MANEX) destinés au personnel d'exploitation[66] et la méthodologie d'intervention sur systèmes opérationnels (MISO) sont rendus obligatoires par la réglementation du ciel unique européen pour exploiter et maintenir un système [technique] ATS, CNS, AIS ou MET. Bien entendu, l'élaboration aussi bien des MANEX que du volet « procédure » d'une MISO repose sur bien d'autres documents requis aussi bien par les règles du prestataire (sur la qualité, la sécurité, la sûreté, etc.) que par l'état de l'art (normes, documents « constructeur », etc.) et autres exigences.



64 Cf. NF EN 15221-1, NF EN 13306, ND 2166 (INRS), « Environnement, sécurité et maintenance » Ed. TI, etc.
65 Cf. FD X60-000, « Optimisation de la maintenance par la fiabilité » Ed. Techniques de l'Ingénieur, etc.
66 « *Air navigation service providers shall provide and keep up-to-date* ***operations manuals*** *relating to the provision of their services for the use and guidance of* ***operations personnel****.* » (REG UE 1035/2011)

Organisation du CESNAC

La division technique assure notamment la **maintenance** : celle-ci est réalisée par des spécialistes. La division CQF est en charge de la **supervision technique** (et de la disponibilité opérationnelle) : **ceci est une spécificité du CESNAC** relativement aux autres sites de la direction des opérations. L'organisation du CESNAC est fixée par la décision DSNA/D n° 05-0043 du 3 mars 2005 portant organisation interne de la direction des opérations :

> **Décision DSNA/D n°05-0043 (modifiée) du 3 mars 2005 portant organisation interne de la DO :**
>
> Le centre d'exploitation des systèmes de la navigation aérienne centraux (CESNAC), dirigé par un chef de centre assisté d'un responsable du système de management intégré, comprend une division exploitation, une division technique et une division communication/qualité de service/formation :
>
> a) La division exploitation est principalement chargée, en temps réel et en temps différé, d'exploiter les systèmes du domaine plan de vol et les réseaux opérationnels nationaux.
>
> b) La **DIVISION TECHNIQUE** est chargée d'assurer l'administration des ***systèmes, des serveurs d'informations et des réseaux***. À ce titre, elle participe à leur installation et mise en service, et elle assure leur **MAINTENANCE** matérielle et logicielle, la gestion de la configuration et l'assistance technique aux clients ;
>
> c) La **DIVISION COMMUNICATION / QUALITÉ DE SERVICE / FORMATION** est chargée de la communication interne et externe, de la gestion de la qualité de service, de la **DISPONIBILITÉ OPÉRATIONNELLE** et de la **SUPERVISION TECHNIQUE** des ***systèmes, serveurs d'informations et réseaux et de la formation initiale et continue des personnels***.

Les fiches de poste des superviseurs techniques multiqualifiés et des responsables de supervision opérationnelle désignent leur chef de subdivision technique comme supérieur hiérarchique direct, ce qui ne pose aucune difficulté particulière, puisque l'ingénieur de permanence représente le chef de la division technique[67]: l'astreint technique[68] peut ainsi donner des ordres à un permanent technique.

Les activités de l'entité QS/DO du CESNAC sont normalement… les suivantes[69] :

- ✔ assurer le traitement des événements Sécurité et Qualité ;
- ✔ assurer la diffusion des enseignements du retour d'expérience (REX) ;
- ✔ produire et alimenter la synthèse Sécurité/Qualité (indicateurs, bilans, publications, …) ;
- ✔ organiser le suivi Sécurité/Qualité (dérives indicateurs, réalisation des actions / ACAP, …) ;
- ✔ constituer le « référent méthode » de la division technique pour la réalisation des études de sécurité (EPIS, MISO, …)[70] ;
- ✔ organiser et animer la gestion de l'information, en particulier vers les superviseurs, à travers les briefings, le **MANEX T**, etc. ;
- ✔ gérer et suivre l'environnement technique de la supervision ;
- ✔ assurer la maintenance spécialisée de la supervision technique centralisée (STC).

C'est normalement… au travers du manuel d'exploitation « technique » que la division CQF fournit les procédures d'exploitation au STM et au RSO assurant la supervision technique au CESNAC[71].

67 Décision SCTA n° I 040003 relative à la mise en œuvre des textes relatifs à l'astreinte au sein du SCTA
68 Arrêté du 26 novembre 2003 (modifié) fixant la liste des astreintes mises en place au sein de la DGAC
69 Référentiel Métier et Compétences QST/DO – v1.1 20/07/2011 – réf. GEODe : DSNA/110913/0003
70 Autrement dit, ils sont les experts désignés pour vérifier les EPIS, les MISO, etc.
71 L'élaboration des procédures étant – bien entendu – une activité nécessitant le support de la division technique.

Auto-maintenance

La norme NF EN 13306 définit l'**auto-maintenance** comme une « maintenance exécutée par un utilisateur ou un personnel d'exploitation » : c'est ce qui la rend particulière. La norme FD X60-000 lui consacre un paragraphe et définit précisément les ***actions de maintenance*** correspondantes :

> — surveillance de l'état du bien et des paramètres significatifs de cet état ;
> — actions prédéfinies de maintenance sur des éléments facilement accessibles **en toute sécurité** (suivant procédure, instructions de maintenance) ;
> — rétablissement provisoire d'une fonction requise par des opérations simples de dépannage (niveau 1).

La norme prévoit la possibilité d'une maintenance palliative accessible au personnel d'exploitation, mais limitée au 1er niveau de maintenance (attention aux « exigences de sécurité » des ANSP). Dans ce même paragraphe, cette norme rappelle ce que sont les ***actions d'exploitation*** dans ce contexte :

> — surveillance d'exploitation du bien ;
> — permutation d'équipements redondants[72] et remise en cycle.

Manuel d'exploitation (MANEX) et plan d'urgence

Notre manuel de management[73] dispose que les non-conformités relatives aux services CNS (ATS ?) fassent l'objet du « traitement curatif » prévu dans les procédures du MANEX des superviseurs :

> Les non conformités relatives aux services ATS détectées par des systèmes automatiques, les contrôleurs aériens ou les pilotes, telles que le non-respect d'une séparation minimum entre 2 aéronefs ou les constats de délais importants font l'objet d'un traitement curatif immédiat, selon les procédures figurant dans les ***manuels d'exploitation*** **des services exploitation** (MANEX).
>
> **L'application des exigences sécurité est prioritaire sur toute autre exigence.**
>
> Les non conformités relatives aux services CNS, telles que l'indisponibilité, la non précision ou la non intégrité des données de communication, de navigation ou de surveillance, détectées par les agents, les pilotes d'aéronef, ou par des systèmes automatiques de supervision[74], font l'objet d'un traitement curatif conformément aux procédures figurant dans les ***manuels d'exploitation*** **des services techniques et exploitation**.
>
> La précision et l'intégrité des données fournies par les systèmes de contrôle sont maîtrisées […] : pour l'ensemble des systèmes CNS […] par une supervision[75] temps réel[76].

Conformément au règlement d'exécution n° 1035/2011, en cas d'**indisponibilité** importante, voire totale, du service rendu, ce sont les procédures du **plan d'urgence** qui doivent être appliquées[77].

> La DSNA dispose d'un ensemble de dispositions et de procédures opérationnelles ayant pour objectifs d'assurer la sécurité en cas d'indisponibilité importante, voire totale, du service rendu, en matière ATS, CNS ou AIS. Ces dispositions sont décrites dans : Plan d'urgence de la DSNA

72 Appelée aussi basculement « normal / secours ». Lorsque la bascule n'est pas automatique, un opérateur est requis.
73 Nous parlons bien de celui de la DSNA. La multiplicité des manuels de management que les agents de la DSNA doivent suivre au quotidien ne leur facilite pas les choses : elle les prive d'une véritable compréhension du SMI.
74 Le système CAUTRA est pourtant supervisé… L'absence de cette mention pour les services ATS est étonnante.
75 Cette rédaction laisse entendre que les systèmes utilisés pour les services de la circulation aérienne (ATS), en particulier les systèmes de traitement des données de vol, les systèmes de traitement des données de surveillance et les systèmes d'interface homme-machine ne feraient pas l'objet d'une supervision technique.
76 Rappelons qu'une supervision (active) est nécessairement en temps réel : elle l'implique.
77 Le plan d'urgence de la DSNA précise d'ailleurs que les procédures d'urgence doivent avoir été intégrées dans le manuel d'exploitation (ou « MANEX »).

La sécurité aérienne du point de vue de la hiérarchie des normes

Il n'est pas question de faire ici un cours de droit, mais rappelons succinctement comment est régi la sécurité du point de vue de la hiérarchie des normes ***pour ce qui concerne les agents de la DSNA***.

Constitution française de 1958 (sommet de la hiérarchie des normes)	1958
Traité sur le fonctionnement de l'Union (traité de Rome)	1957
Traité instituant la Communauté européenne (traité de Lisbonne) « *les traités et le droit adopté par l'Union sur la base des traités priment le droit des États membres* »	2009
Loi n° 63-69 du 30 janvier 1963 autorisant la ratification de la convention « Eurocontrol »	1963
Décret n° 63-332 du 19 mars 1963 portant publication de la convention Eurocontrol[78]	1960
AG (ex « commission permanente pour la sécurité de la navigation aérienne »)	1960
Décision n° 87 portant approbation de l'ESARR 4 en vue de son intégration effective dans les cadres réglementaires relatifs à l'ATM des États membres d'Eurocontrol	2001
ESARR 4 « Évaluation et atténuation des risques dans le domaine ATM » « *La présente exigence s'applique à l'ensemble des prestataires de services ATM pour ce qui concerne les sous-ensembles du système ATM et les prestations de support dont ils assurent la gestion.* » / « *Cette exigence doit être vérifiée quels que soient les arrangements institutionnels nationaux ou internationaux qui permettent la fourniture des services ATM.* » / « ***Aucune dispense n'est prévue.*** »	2001
Ciel Unique Européen : cadre pour la réalisation du CUE / REG CE n° 549/2004	2004
Ciel Unique Européen : règles de l'UE sur les services de N.A. / REG CE n° 550/2004 « *Article 4 - Exigences de sécurité* *Conformément à la procédure visée à l'article 5, paragraphe 3, du règlement-cadre, la Commission identifie et adopte les* ***exigences réglementaires de sécurité d'Eurocontrol*** ***(ESARR) ainsi que leurs modifications ultérieures dans le cadre du présent règlement, exigences dont le respect est imposé par la législation communautaire****. Les références de ces ESARR sont publiées au Journal officiel de l'Union européenne.* » (voir le principe ICI)	2004
REG UE n° 1035/2011 établissant des exigences communes pour la fourniture de SNA	2011
REG CE n° 482/2008 établissant un système d'assurance de la sécurité des logiciels	2008
Gouvernement français : codes, décrets, arrêtés, circulaires, etc.	
DSNA (SMI) « *Tout changement apporté au système[79] ATM/CNS (procédures, facteurs humains[80], équipements) fait l'objet d'une évaluation des risques associées, du point de vue de la sécurité, afin d'atténuer ces risques par anticipation.* »	2006
Procédure pour l'évaluation et l'atténuation des risques (PRO_002)	2005
Méthodologie pour l'évaluation et l'atténuation des risques (MET_001)	2008
Méthodologie de traitement des logiciels (MET_006)	2009
Manuel ÉPIS-TIL, manuel ÉPIS-CA, manuel MISO, etc.	

78 Formellement : convention internationale de coopération pour la sécurité de la navigation aérienne « Eurocontrol »
79 Cette rédaction est obsolète : l'expression à utiliser aujourd'hui est « … aux systèmes fonctionnels ATM/CNS … ».
80 L'emploi ici de cette expression est inappropriée : il faut plutôt parler de « ressources humaines ».

Réglementation du ciel unique européen et exigences de sécurité

La réglementation du Ciel unique impose aux prestataires ANS le respect d'**exigences de sécurité**. Elle précise que le « basculement » ou le « remplacement à chaud » d'un composant matériel, d'un programme informatique ou bien des données de configuration de celui-ci doit **systématiquement** faire l'objet d'une identification des dangers ainsi que d'une évaluation et atténuation des risques.

« **système fonctionnel** » : une combinaison de systèmes [techniques], de procédures et de ressources humaines organisée *afin de remplir* ***une fonction*** *dans le contexte de la gestion du trafic aérien* (REG UE 1034/2011, REG UE 1035/2011, REG CE 482/2008)

« **système [technique]** » : le regroupement des composants au sol et embarqués, ainsi que des équipements spatiaux, qui fournissent un appui aux services de navigation aérienne pour toutes les phases de vol (REG CE 549/2004)

« **composants** » : les objets tangibles, tels que le matériel, et les objets intangibles, tels que les logiciels, dont dépend l'interopérabilité du réseau européen de gestion du trafic aérien (REG CE 549/2004)

« logiciels » : les programmes informatiques et les données de configuration correspondantes, y compris les logiciels prédéveloppés, à l'exclusion des éléments électroniques tels que les circuits intégrés spécifiques d'une application, les réseaux de portes programmables ou les dispositifs de contrôle de logique sur support physique (REG CE 482/2008)

« **basculement ou remplacement à chaud** » : le remplacement d'un composant ou d'un logiciel du système du réseau européen de gestion du trafic aérien (EATMN) pendant que le système [technique] est opérationnel (REG CE 482/2008)

TOUTE MODIFICATION DES SYSTÈMES FONCTIONNELS doit […] faire l'objet d'une supervision de la sécurité (REG UE 1034/2011)

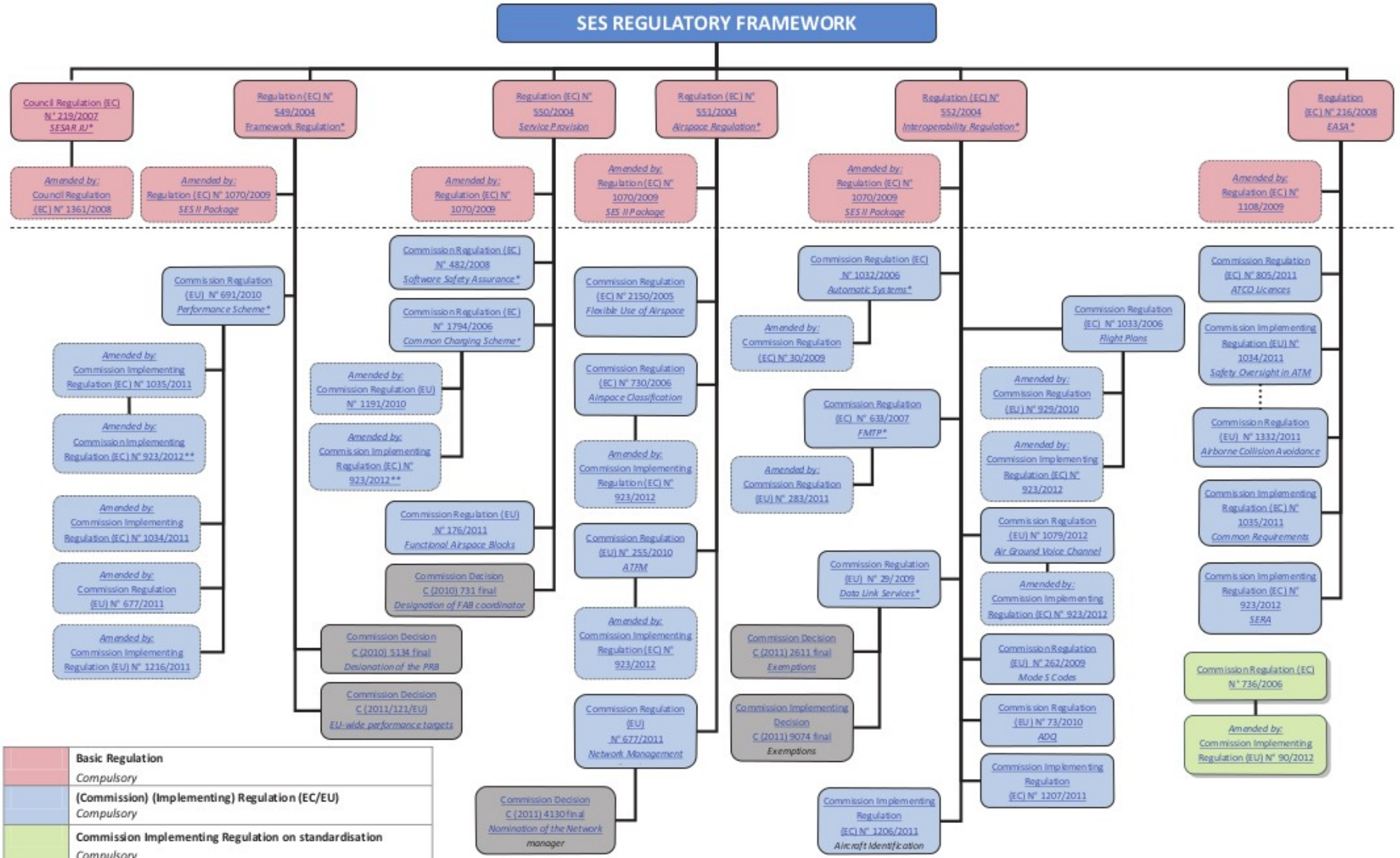
Le prestataire élabore des procédures permettant de gérer la sécurité […] lors de la **MODIFICATION DE SYSTÈMES FONCTIONNELS** (REG UE 1035/2011)

le prestataire […] s'assure que l'évaluation des risques et leur atténuation sont menées au niveau approprié afin que **TOUS LES ASPECTS** de la fourniture des services de gestion du trafic aérien soient bien pris en compte (**évaluation des risques et leur atténuation**). Pour les **modifications apportées au système fonctionnel** de gestion du trafic aérien, le point 3.2 s'applique (REG UE 1035/2011)

3.2) le prestataire [...] veille à ce que l'identification des dangers ainsi que l'évaluation et l'atténuation des risques soient **SYSTÉMATIQUEMENT EFFECTUÉES** [...] d'une manière qui couvre [...] **L'INTÉGRALITÉ DU CYCLE DE VIE** du sous-ensemble considéré du système fonctionnel de gestion du trafic aérien, [...] **Y COMPRIS LA MAINTENANCE** / Les résultats, justifications et éléments de preuve découlant des processus d'évaluation et d'atténuation des risques, y compris l'identification des dangers, doivent être rassemblés et documentés / Une identification systématique des dangers doit être effectuée. (REG UE 1035/2011)

Lorsqu'une organisation doit mettre en œuvre un processus d'évaluation et d'atténuation des risques en vertu du droit communautaire ou national applicable, elle définit et met en œuvre un système d'assurance de la sécurité des logiciels portant spécifiquement sur les aspects liés aux logiciels EATMN, **Y COMPRIS L'ENSEMBLE DES MODIFICATIONS OPÉRATIONNELLES APPORTÉES EN LIGNE, ET NOTAMMENT LES BASCULEMENTS OPÉRATIONNELS OU LES REMPLACEMENTS À CHAUD**. (REG CE 482/2008)

Le présent règlement est **OBLIGATOIRE DANS TOUS SES ÉLÉMENTS** et **DIRECTEMENT APPLICABLE** dans tout État membre. (REG UE 1034/2011, REG UE 1035/2011, REG CE 482/2008)



* Consolidated Version

** Not included in the consolidated version

Application des exigences de sécurité du Ciel unique à la DSNA

Procédure pour l'évaluation et l'atténuation des risques (PRO_002) :

Cette procédure précise l'organisation de la DSNA pour la gestion des changements du **système fonctionnel** DSNA[81].

La présente procédure s'applique lors de l'introduction, à titre permanent ou temporaire, de nouveaux **systèmes fonctionnels** ou lors de la modification de **systèmes fonctionnels** existants.

La notion de **système fonctionnel** est définie (cf. [Réf. 1]) de la façon suivante : une combinaison de **systèmes (équipements techniques)**, de **procédures** et de **ressources humaines** organisée afin de remplir une fonction dans le contexte de la gestion du trafic aérien.

Pour la DSNA, cette procédure s'applique donc pour tout changement d'au moins une des composantes (**procédures**, **facteurs humains**, **équipements**) du **système fonctionnel** ATM/CNS/AIS relevant des missions de la DSNA à l'exception des changements organisationnels ou managériaux, ainsi que les prestations de support dont la DSNA assure la gestion.

Il peut s'agir de l'introduction d'un nouveau **système fonctionnel**, de la modification d'un **système fonctionnel** existant, **y compris si cette modification est temporaire**, ou d'une intervention programmée sur un équipement opérationnel.

Elle ne concerne pas les interventions en réaction immédiate à des défaillances[82].

3. DOCUMENTS DE RÉFÉRENCE

3.1. Documents applicables

[Réf. 1] Règlement d'exécution de l'Union Européenne n°1035/2011 du 17 octobre 2011 établissant les exigences communes pour la fourniture de services de navigation aérien

[Réf. 2] Règlement d'exécution de l'Union Européenne n°1034/2011 du 17 octobre 2011 sur la supervision de la sécurité dans la gestion du trafic aérien et les services de navigation aérienne

[Réf. 3] Règlement (CE) No 482/2008 du 30 mai 2008 établissant un système d'assurance de la sécurité des logiciels à mettre en œuvre par les prestataires de services de navigation aérienne.

Il reste encore des IESSA, attachés à une certaine vision de leur métier, ne faisant pas grand cas des exigences de sécurité du ciel unique européen. À l'occasion d'un grave incident en 2008, ceci a forcé le DSNA à réagir très fortement. Ils s'appuient parfois sur cette phrase de la PRO_002 « *Elle ne concerne pas les interventions en réaction immédiate à des défaillances* » pour justifier de ne pas procéder à une étude de sécurité lors d'interventions sur les systèmes opérationnels. Et ce, avec le soutien d'un encadrement qui, pour autant, évite bien d'expliciter cela par des ordres exempts de toute ambiguïté. De quelle défaillance parle t-on ici ? Est-ce que la "défaillance" d'un témoin lumineux, d'une jarretière, d'un câble coaxial, d'un équipement, etc. peut justifier d'intervenir sur un système en cours d'utilisation pour le réparer sans évaluation/atténuation des risques ou sans coordination ? Cette vision est en **contradiction absolue** avec les exigences de sécurité. Pour comprendre la signification de cette phrase, a priori détonante, il faut interpréter cette procédure (comme les autres) à l'aune du cadre réglementaire cité en référence. Il s'agit de la **défaillance d'une fonction ATM/CNS** (cf. arrêté du 17 août 2007 fixant la liste d'événements et d'incidents d'aviation civile, etc.), la seule défaillance impactant l'interface pilote/contrôleur. Autrement dit, la perte totale ou partielle d'un service support : terme historique pour désigner une fonction opérationnelle (une fonction ATM/CNS), mais qui tombe en désuétude.

81 Il n'y a pas un système fonctionnel à la DSNA, mais plusieurs : un système par fonction opérationnelle.
82 Il s'agit des défaillances d'un système fonctionnel (ie : défaillances vues de l'interface pilote/contrôleur).

Méthodologie pour l'évaluation et l'atténuation des risques … (MET_001) :

Ce document définit la méthodologie DSNA pour la réalisation des études d'évaluation et d'atténuation des risques qui doivent être réalisées **avant tout changement** du système fonctionnel DSNA, incluant, dans ce contexte, les domaines ATM, CNS et AIS. Dans la suite de ce document, ce système intégrant les domaines ATM, CNS et AIS est appelé « système fonctionnel DSNA ».

Il complète la procédure pour l'évaluation et l'atténuation des risques appliquée par la DSNA **pour répondre à l'annexe II - § 3.2 du Règlement UE n°1035/2011 du 17 octobre 2011** établissant les exigences communes pour la fourniture de services de navigation aérienne.

Ce document est complété par la « Méthodologie de traitement des logiciels » MET_006/DSNA qui décrit les dispositions à prendre pour l'évaluation et l'atténuation des risques liés aux logiciels. Il convient de se référer à ce document MET_006/DSNA **dès lors qu'un ou plusieurs logiciels sont impactés par le changement**.

La réglementation en vigueur **impose** qu'une procédure d'évaluation et d'atténuation des risques soit **SYSTÉMATIQUEMENT CONDUITE** pour tout changement apporté dans le système fonctionnel DSNA et à des prestations de support, c'est-à-dire que **chacun de ces changements fasse l'objet d'une étude de sécurité**.

L'approche pour l'évaluation et l'atténuation des risques consiste en la réalisation d'une étude de sécurité qui couvre :

- ➔ **L'INTÉGRALITÉ DU CYCLE DE VIE** du sous-ensemble considéré du système fonctionnel DSNA, des phases initiales de planification à sa mise en œuvre, **Y COMPRIS LA MAINTENANCE** et éventuellement le retrait du service,
- ➔ les trois éléments constitutifs du système fonctionnel DSNA, à savoir les **équipements**, les **procédures** et les **ressources humaines**, leurs interactions ainsi que les interactions entre le sous-ensemble considéré et les autres constituants du système fonctionnel DSNA, dans un environnement opérationnel donné,
- ➔ les composantes sol et air (y compris la composante spatiale) du système fonctionnel DSNA, à travers une coopération avec les organismes compétents.

Les changements sont étudiés en prenant en compte l'environnement opérationnel. Ils peuvent concerner tout ou partie des 3 domaines suivants :

- **LES ÉQUIPEMENTS** (matériel et logiciel) :
  - installation et utilisation d'un nouvel équipement,
  - modification d'un système existant[83],
  - intervention programmée,
- **LES PROCÉDURES** suivies par les agents opérationnels dans l'accomplissement de leurs fonctions liées à la fourniture de service ATM/CNS, par exemple :
  - modification de l'espace aérien (modification de la sectorisation, nouvelles trajectoires avec procédures associées, etc.),
  - modification des procédures opérationnelles[84], etc.
- **LES RESSOURCES HUMAINES** : toute interaction de l'humain avec les éléments du système fonctionnel DSNA (méthodes de travail, charge de travail, gestion IHM, application des consignes, etc.).

83 « **y compris l'ensemble des modifications opérationnelles apportées en ligne** » (REG CE 482/2008)
84 Sans oublier leur introduction !

SMS DSNA et interventions programmées

Le SMS de la DSNA est sans ambiguïté sur ce point : toute intervention programmée qui pourrait impacter une fonction opérationnelle[85] doit impérativement faire l'objet de la **« procédure MISO »**.

Procédure pour l'évaluation et l'atténuation des risques (PRO_002) :

LES INTERVENTIONS PROGRAMMÉES concernant les équipements opérationnels du système ATM/CNS **FONT L'OBJET D'UNE PROCÉDURE SPÉCIFIQUE** : la **procédure MISO**.

Il est rappelé que la méthodologie de traitement des logiciels (MET_006) s'applique aussi pour les interventions programmées.

Méthodologie pour l'évaluation et l'atténuation des risques … (MET_001) :

Les ÉTUDES DE SÉCURITÉ relatives aux INTERVENTIONS PROGRAMMÉES sont cadrées par la **procédure « MISO »** (Méthodologie d'Intervention sur Systèmes Opérationnels).

Celle-ci s'applique AUX INTERVENTIONS PROGRAMMÉES, qu'elles soient :

- **d'origine interne** : intervention par les services de la DSNA impactant ou susceptible d'impacter les équipements opérationnels du système fonctionnel DSNA qui relèvent de sa responsabilité

ou

- **d'origine externe** : intervention par un prestataire externe (exemple opérateur Télécom) ayant un impact sur les équipements opérationnels de la DSNA. Dans ce cas la DSNA, en lien avec le prestataire extérieur, évalue l'impact de cette intervention, en utilisant MISO.

Les MISO sont uniquement liées aux phases **ponctuelles** d'interventions, réglages, etc. sur des équipements.

Guide d'utilisation MISO (version actuelle et version à venir) :

Ce document définit la Méthodologie d'Intervention sur Systèmes Opérationnels (MISO) pour l'évaluation-atténuation des risques avant **TOUTE INTERVENTION PROGRAMMÉE** [sur/impactant] un équipement technique du système ATM/CNS.

SMS DSNA et maintenance corrective

Méthodologie pour l'évaluation et l'atténuation des risques … (MET_001) :

[…] **les interventions programmées ne nécessitant « qu'une » MISO** […]

A : **Changement de composant simple (matériel et/ou logiciel)**

B : Modification de contexte opérationnel

C : **Modification de paramétrage**

D : Intervention uniquement liée à l'environnement du système ou de la chaîne

E : Réorganisation géographique d'équipements

F : Maintenance préventive

G : Modification de logiciel[86] qui se limite strictement à de la **maintenance corrective**[87] / Ces cas ne nécessitent pas d'ÉPISTIL. En revanche, les dispositions SASL s'appliquent.

85 Comprendre un service de navigation aérienne (ATS, CNS, …), voire une fonction ATM (ASM, ATFM, ATS).
86 Un logiciel est réglementairement l'association d'un programme informatique et de ses données de configuration.
87 Rappelons que la maintenance palliative est l'une des deux subdivisions de la maintenance corrective.

Méthodologie d'intervention sur systèmes opérationnels (principe)

L'évaluation et l'atténuation des risques est incontournable dans le monde de l'aérien. Celles-ci passent nécessairement et obligatoirement par l'utilisation de procédures pour assurer la Sécurité ; procédures qui font elles-mêmes l'objet d'une amélioration continue dans le cadre de la Qualité[88]. Chaque mission comme l'Exploitation (le contrôle aérien, la conduite technique des systèmes, etc.), la Maintenance et la Sécurité, chaque domaine d'activité et chaque tâche relève de procédures.

Le tableau suivant permet de situer l'activité relative aux maintenances sur les systèmes techniques opérationnels dans ce dédale de procédures et de savoir quand utiliser la procédure MISO :

	Exploitation (traitement curatif et urgence)	**Maintenance** (MCO)	**Sécurité** (supervision de la sécurité)
Obéissance hiérarchique ordre hiérarchique émanant de/du …	**MANEX** (dont le plan d'urgence) approuvé par **l'autorité**	**Formulaire MISO** (volet « Procédure ») approuvé par **l'autorité**	**Ordre oral ou écrit** DSNA **supérieur hiérarchique**
Application du SMS	**Manuels EPIS (-CA, -TIL)** introduction/modification de composants, de procédures, etc.	**Procédure MISO** intervention programmée susceptible d'impact	« **Consigne de sécurité** » condition compromettant la sécurité aérienne
Organisme (SMS)	**DSNA** (PRO_002)		**DSAC** (P_109)
Réglementation	**REG UE 1035/2011** **REG CE 482/2008**		**REG UE 1034/2011**
	REG CE 549/2004, **REG CE 550/2004** (« règlement-cadre » + règlement d'application)		

Rappelons que la DSNA n'est pas officiellement en charge de la sécurité aérienne : cette mission relève de la DSAC. La DSNA est chargée de fournir les services ATS, CNS et AIS[89] : autrement dit, elle est chargée d'assurer l'écoulement régulier des vols dans l'espace aérien qui lui a été confié. Et elle doit le faire en garantissant en priorité la sécurité. Si, pour une raison ou une autre, elle échouait à assurer cet écoulement régulier dans des conditions normales, elle peut basculer en urgence dans un mode opératoire dégradé, mais tout en assurant le même niveau de sécurité. Si la sécurité était impossible à assurer même dans ces conditions, il revient à la DSAC de prendre les dispositions nécessaires : puisque la **supervision de la sécurité** est assurée par celle-ci[90]. Pour le dire autrement, il n'appartient pas réellement à la DSNA de décider de ce qui est dangereux ou pas : pour le savoir, elle doit appliquer les procédures approuvées par la DSAC (ou lui demander directement).

La « procédure MISO » doit être appliquée pour toute intervention programmée « *impactant ou susceptible d'impacter les équipements opérationnels du système fonctionnel DSNA* » (MET_001).

> **Procédure pour l'évaluation et l'atténuation des risques (PRO_002) :**
>
> Les interventions programmées concernant les équipements opérationnels du système ATM/CNS font l'objet d'une procédure spécifique : la **procédure MISO** (Méthodologie d'Intervention sur Système Opérationnel).

Sans doute plus qu'une autre, cette procédure doit faire l'objet d'une très grandeur rigueur dans son application, car les études de sécurité résultantes ne font pas l'objet d'une notification à la DSAC.

88 Le système de gestion de la sécurité en vigueur à la DSNA est une déclinaison du système de gestion de la qualité.
89 Décret n° 2005-200 du 28 février 2005 portant création de la direction des services de la navigation aérienne
90 « Les organismes recourent uniquement à des procédures acceptées par leur autorité compétente pour décider d'apporter à leurs systèmes fonctionnels un changement lié à la sécurité » (REG UE 1034/2011)

Situation de la maintenance relativement au SMI

Notre SMI et en particulier notre SMS, qui y est intégré, empruntent considérablement à l'ISO 9001 et à sa terminologie. Rien que ce sujet pourrait faire l'objet d'un dossier spécifique. À cela, il faut intégrer la réglementation du ciel unique européen (dont les exigences de sécurité), etc. Nous nous contenterons ici de résumer les actions à tenir relativement aux différents types de constat relatif à la sécurité. Dans notre SMI, la maintenance s'inscrit dans le traitement différé des événements dits « de sécurité », ainsi que dans le cadre de l'amélioration continue (ISO 9001). Dans l'état actuel de nos textes[91], voici un tableau résumant les actions à tenir en particulier au CESNAC :

Type de constat[92]	Traitement immédiat	Traitement différé[93]
Non-conformité (ou **écart**)[94] Indisponibilité, non précision ou non intégrité des données	Action curative : **traitement immédiat des événements sécurité**	Action (curative) et/ou ACAP : **traitement différé des événements sécurité**
Indisponibilité importante ou totale d'un service ATS ou CNS[95]	Action curative : **notification (IP), application des procédures d'urgence[96] (STM, IP)**	Action curative : **retour aux opérations en mode normal**
Événement compromettant la sécurité[97]	Notification : **agent → IP → RPO-DO → DSAC** émission possible d'une « consigne de sécurité »	Action curative : **application de la « consigne de sécurité »**
Observation, recommandation ou suggestion[98]	–	**ACAP**

Soulevons un problème de terminologie. Le mot « événement » peut être ambigu : dans notre SMI, il désigne formellement[99] un accident, incident ou tout autre défaut ou dysfonctionnement d'un des « systèmes fonctionnels » de la DSNA ayant pour conséquence de compromettre le niveau de sécurité (ou de sûreté). Il s'agit par conséquent d'événements de catégories ‹ **aa** ›, ‹ **a** › et ‹ **b** ›. Une indisponibilité importante ou totale d'un service ATS ou CNS dans de « bonnes conditions de sécurité » est un événement de catégorie ‹ **c** ›. C'est une situation où il y a une surcharge de travail du personnel de contrôle (des régulations plus ou moins importantes), mais sans aucune atteinte à la sécurité. Les non-conformités (ou écarts) se répartissent dans les catégories restantes : ‹ **d** ›, ‹ **e+** › et ‹ **e** ›. Toutefois, on doit prendre garde que si une non-conformité aboutissait à un accident aérien, cette circonstance sera affectée de la classe la plus grave, autrement dit ‹ **aa** ›. Ce classement se fait *a posteriori* bien entendu (il est à rapprocher du niveau de gravité *a priori* des études de sécurité).

91 Procédure de traitement des constats et des ACAP (PRO_003), procédure DO de traitement des événements de sécurité, manuel de traitement des événements « sécurité » par les services techniques, note de service n° 12/008/CESNAC du 17 février 2012 et procédure CESNAC de traitement des événements de sécurité (Pg011)
92 Concernant le traitement des événements dit de sécurité (au sens large), sans pour autant compromettre la sécurité.
93 « Le traitement différé des événements est réalisé au niveau local avec appui de l'échelon central de la DO. »
94 Ex : non-respect d'une séparation minimale, retards, indisponibilité, non précision, non intégrité des données, etc.
95 Face à l'absence d'information de la DSNA envers ses agents, on peut considérer que le système fonctionnel inclut ses procédures d'urgence et leur application par le personnel formé à une telle situation : le système fonctionnel fonctionne… Il n'est pas défaillant. Surtout si la sécurité n'était pas compromise par l'application du plan d'urgence.
96 On passe dans un mode de fonctionnement dit dégradé, mais prévu, où la sécurité n'est ni dégradée ni compromise.
97 Défaillance d'un « système fonctionnel ».
98 Les sources des constats sont les suggestions des agents, les dérives constatées via le suivi des indicateurs (pilotage des processus SMI), les résultats des audits internes et externes, les préconisations de la DSAC, d'Eurocontrol, etc.
99 Cf. procédure de traitements des constats et des ACAP (PRO_003)

Ainsi, dans un cadre de travail quotidien des IESSA, ceux-ci effectuent les actions curatives prévues dans leur manuel d'exploitation lorsqu'ils assurent la permanence technique (traitement curatif). Ils sont également sollicités pour réaliser des maintenances dans le cadre d'un traitement différé des non-conformité détectées par la supervision technique. Ce que nous allons rappeler très brièvement.

Traitement immédiat des événements « sécurité »

STM : report des événements (PV)
STM : analyse initiale
STM : traitement curatif via les procédures normales[100]
IP : notification immédiate si nécessaire
IP : mesures conservatoires si nécessaire

Traitement différé des événements « sécurité »

QS/DO : collecte (PV), tri des constats, notification, analyse[101]
QS/DO (GLST) : décision action (en GLST), mise en œuvre (acteurs divers), suivi
division CQF (CLS) : vérification, CRDT, REX
action : autre action curative (maintenance corrective, etc.), transfert du constat et/ou ACAP

PV → QS/DO (tri) → GLST (décision) → action (MS, ACAP, etc.) → CLS (vérification) → CRDT → REX (agents)[102]

Procédure DO de traitement des événements sécurité :

Au sein du CESNAC, la Subdivision Qualité de Service est chargée du traitement des **événements ATM de type dysfonctionnement des systèmes opérationnels et/ou facteurs humains associés**.

Amélioration continue (ACAP)

Action corrective
(amélioration continue)
L'élimination de la cause d'une non-conformité

Action corrective
(amélioration continue)
La prévention des non-conformités

<table>
<tr><td colspan="3">Exploitation
Temps réel : contrôle, conduite, urgence, auto-maintenance</td><td>Maintenance
Intervention programmée</td></tr>
<tr><td>Contrôleurs aériens
Permanence contrôle</td><td>Superviseurs techniques
Permanence technique</td><td>Spécialistes
Renfort « MO »[103]</td><td>Spécialistes
Maintenance spécialisée</td></tr>
<tr><td>MANEX EXP</td><td colspan="2">MANEX TECH</td><td>Volet Procédure de la MISO</td></tr>
<tr><td>EPIS-CA</td><td colspan="2">(liste des interventions de conduite des systèmes NA)
EPIS-TIL</td><td>MISO
(SASL, EPIS-TIL, IOP, …)</td></tr>
<tr><td colspan="4">Réglementation, SMI, exigences, normes, documents techniques, expression du besoin, etc.</td></tr>
</table>

100Dont la notification immédiate de certains événements.
101« Chaque jour, la subdivision QS analyse les journaux de bord superviseurs » (Pg011)
102« Le REX vise ... à largement diffuser les enseignements au niveau local et national » (manuel TES)
103Certains sites auraient mis en place un renfort de la MO pour pallier à la surcharge de travail des superviseurs.

Différentes modalités d'application de la procédure « MISO »

MISO mono-site	Organisme
Volet Technique (service Technique)	1) Description ? 2) MRR ?
Communication technique/exploitation	↓
Volet Exploitation (service Exploitation)	3) Points d'impacts ? 4) ER ? 5) MRR ? **6) Gravité ?**

La procédure MISO est une étude de sécurité. Elle se conclut systématiquement et inéluctablement par une **évaluation du niveau de gravité de l'intervention** en tenant compte de tous les risques liés (aléas, échec de l'intervention, etc.), des MRR (en prévention et en protection) prévus, etc.

« L'identification des dangers ainsi que l'évaluation et l'atténuation des risques comprennent ... l'évaluation des incidences potentielles ... sur la sécurité des aéronefs, ainsi qu'une **évaluation de la gravité** » CUE

MISO multi-sites	Organisme « intervenant »	Communication inter-sites	Organisme « client »
Volet Technique (service Technique)	1) Description ? 2) MRR ?	projet de travaux →	pas de réponse attendue
Communication technique/exploitation	↓	(I)nformation	
Volet Exploitation (service Exploitation)	3) Points d'impacts ? 4) ER ? 5) MRR ? **6) Gravité ?**		

MISO multi-sites	Organisme « intervenant »	Communication inter-sites	Organisme « client »
Volet Technique (service Technique)	1) Description ? 2) MRR ?	projet de travaux →	3) Description ? 4) MRR ?
Communication technique/exploitation		(C)oncertation	↓
Volet Exploitation (service Exploitation)	Pas de volet Exploitation en propre, mais **synthèse locale à faire**	Formulaire MISO de l'organisme client ← pour synthèse locale	5) Points d'impacts ? 6) ER ? 7) MRR ? **8) Gravité ?**

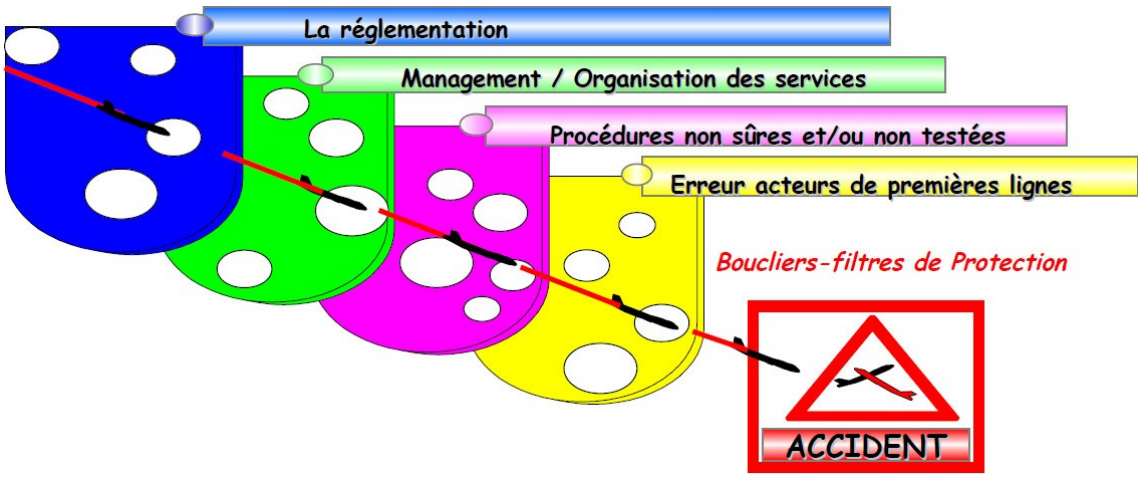
MISO multi-sites	Organisme « intervenant »	Communication inter-sites	Organisme « client »
Volet Technique (service Technique)	1) Description ? 2) MRR ?	projet de travaux →	3) Description ? 4) MRR ?
Communication technique/exploitation	↓	(C)oncertation	↓
Volet Exploitation (service Exploitation)	9) Points d'impacts ? 10) ER ? 11) MRR ? **12) Gravité ?**	Formulaire MISO de l'organisme client ← pour synthèse locale	5) Points d'impacts ? 6) ER ? 7) MRR ? **8) Gravité ?**

Modèle des plaques (ou du « fromage suisse ») de Reason

La seule manière permise de procéder à une maintenance corrective immédiate repose sur une **procédure opérationnelle** (ou via une consigne de sécurité). L'introduction de cette procédure dans un système fonctionnel est un changement, mais pas son exécution par le personnel qualifié. Même si toute maintenance est dangereuse, particulièrement la maintenance palliative, l'étude de sécurité subséquente sera à même de décider la pertinence d'introduire une action corrective de cette nature dans l'enveloppe fonctionnelle du système concerné. Rappelons encore que les basculements et les remplacement à chaud d'un composant matériel, d'un programme informatique ou des données de configuration de celui-ci doivent **systématiquement** faire l'objet d'une identification des dangers ainsi que d'une évaluation et atténuation des risques ; que l'indisponibilité d'un service CNS doit faire l'objet d'un traitement curatif conformément aux procédures figurant dans les MANEX. En cas d'indisponibilité importante, voire totale, du service ATM/CNS rendu, on doit appliquer les procédures du MANEX relatives au plan d'urgence (mode dégradé). Et si l'autorité de surveillance le jugeait nécessaire, elle pourrait encore émettre une consigne de sécurité pour rétablir la sécurité.

Ainsi, rien ne peut et ne doit déroger aux exigences de sécurité définies par la réglementation. Cet aspect « systématique » est conforme aux principes définis par James Reason pour apporter une solution aux accidents dus aux **erreurs de nature organisationnelle**. Voici ce qui finit par arriver en l'absence d'un « **système de gestion de la sécurité** » :

Modèle de Reason (« *Swiss Cheese Model* »)[104] :



James Reason a fondé son célèbre modèle sur la base des tenants organisationnels des mécanismes de l'erreur humaine. Un « **système de gestion de la sécurité** » ou SGS, appelé également SMS, est conçu pour éviter les « trous » dans une organisation (voire l'alignement des trous résiduels) qui aboutiraient fatalement à l'accident. C'est l'objet même d'un SGS (ou SMS). Les ESARR, comme les « exigences de sécurité » du « Ciel unique » et notre SMS sont bâtis notamment sur ce modèle. Le SMS doit par exemple permettre d'améliorer les procédures mais également veiller à la bonne compréhension de celles-ci par le personnel concerné[105]. L'amélioration se traduit par des actions correctives et préventives (ou ACAP) au sens de la norme ISO 9001.

Attention : si un traitement curatif ou une maintenance corrective peuvent être considérées comme des actions correctives au sens usuel du terme, ce ne sont pas nécessairement des actions correctives au sens de l'ISO 9001. Si l'action était déjà prévue dans une procédure, ce n'est pas une « ACAP ».

104« Revisiting the "Swiss Cheese Model of Accidents » Eurocontrol
105Les procédures doivent être intelligibles : elles doivent être comprises par les agents chargés de les appliquer.

Menace de sanctions contre les IESSA par le DSNA (en 2008)

Il n'est pas inutile de rappeler ici les menaces émises en 2008 par le DSNA envers les IESSA qui ne respecteraient pas l'obligation de programmer sous MISO toute maintenance qui pourrait impacter un système opérationnel.

Acte 1 : deux incidents techniques ayant eu des conséquences graves sur les vols

Panne radio du 19 février 2008 :

« *Ce dysfonctionnement a eu pour effet la coupure des émetteurs secours (du CER local).*

Suite à l'installation d'une nouvelle antenne intégrée fin 2007, 3 fréquences ont été déplacées sur cette antenne en janvier 2008. Par la suite 3 autres fréquences ont été ajoutées à cette antenne début février. A chaque fois une MISO a été instanciée pour ces opérations.

Un produit d'intermodulation est alors apparu.

La section Radiocom entreprend alors de résoudre le problème. ***Elle considère être dans un schéma de correctif de panne. (pas de MISO)*** »

« *Concernant les aéronefs il y a eu*

- *2 vols retardés*
- *2 appareils sont passés sur fréquence de détresse)*
- *1 des vols s'est posé sans fréquence (atterrissage sans autorisation).*

La situation a été mal vécue par les contrôleurs qui ne maîtrisaient pas du tout la situation. »

Panne radio du 10 avril 2008 :

« *Une baie fibre optique est en cours d'installation au CRD. Une intervention est programmée pour des mesures de continuité dans les baies fibre optique.* ***Il s'agit donc de matériel non encore opérationnel en cours d'installation (sans MISO puisque baies non opérationnelles)***. »

« *Pour la fréquence AE (IFR) il y a eu perte de réception de 13h23:25 jusqu'à 13h25:29 puis de 13h27 :05 jusqu'à 13h27 :20 concernant Soit un total temps cumulé de 2'19"de coupure.*

Un seul avion (EZY 6139) a été concerné.

Pour le LOC il y a eu perte de réception avec 2 conflits au sol puis ensuite 1 conflit en l'air (les avions revenant sur la fréquence 118.100 ceci combiné à une situation orageuse).

Toulouse a procédé à des arrêts de décollage et demandé au CRNA-SO de garder les avions en fréquence.

Les VHF du CRNA-SO ont basculé sur les fréquences secours et les 2 fréquences UHF ont été temporairement HS.

Globalement la situation s'est avérée difficile avec un trafic dense et compliqué (parachutages, avions SEFA en entraînement) et une situation météo orageuse avec, de plus, un élève contrôleur en position IFR. »

Ces citations sont extraites du CR du séminaire QST-DO des 25 et 26 novembre 2008.

Acte 2 : menace de sanctions du DSNA

Courrier DSNA/D – N° 080920 (16 juillet 2008) :

« Je constate dans les deux cas deux manquements graves à des obligations de sécurité :

- **absence de procédure mise**[106] en infraction avec la note de service 2006/00062/SNA/S/TA/DO ;

- **absence de coordination** avec le CDI pendant les opérations en infraction avec la note de service 2006/00061/SNA/S/TA/DO. »

« Je vous demande donc d'insister auprès de l'ensemble des services de la direction des opérations sur l'**impérative nécessité de respecter les notes et procédures** applicables en matière d'interventions techniques en indiquant que **TOUT MANQUEMENT SERA SANCTIONNÉ**. »

2006/00061/SNA/S/TE/DO :

« 1 – Toute intervention prévue sur matériel en service opérationnel doit faire l'objet d'une information préalable au Superviseur (planning demande de travaux MISO, MESO).

2 – L'harmonisation des informations du Chef de Tour (fiche Secteur) et celles du Superviseur (planning demande de travaux…) se fera par un contact en Vigie en début de journée.

3 – Avant de débuter l'intervention le Superviseur en informe le Chef de Tour.

4 – A la fin de l'intervention le Superviseur remet au Chef de Tour l'équipement. »

2006/00062/SNA/S/TE/DO :

« **Toute intervention sur un matériel opérationnel doit faire l'objet d'une demande de travaux ou d'une étude d'évolution**[107] **et d'atténuation du risque telle que définie dans la PROCÉDURE MISO**[108].

Le rédacteur de la de la[109] MISO sera le responsable de l'opération.

Il sera désigné en réunion « service technique » du jeudi matin. »

Il semble difficile d'être plus clair[110]. Et ce rappel à l'ordre est bien conforme tant avec l'ESARR 4 qu'avec les exigences des textes nationaux et européens (REG 1035/2011, etc.) qui l'ont intégré.

Décision n° 87 portant approbation de l'Exigence réglementaire de sécurité EUROCONTROL (ESARR 4) intitulé « Évaluation et atténuation des risques dans le domaine ATM »

La Commission permanente pour la sécurité de la navigation aérienne,

Vu la Convention internationale de coopération pour la sécurité de la navigation aérienne « EUROCONTROL » ...

prend la décision suivante :

La Commission approuve, **en vue de son intégration effective dans les cadres réglementaires relatifs à l'ATM des États membres d'EUROCONTROL**, l'Exigence réglementaire de sécurité EUROCONTROL (ESARR 4) intitulé « Évaluation et atténuation des risques dans le domaine ATM », élaborée par la Commission de réglementation de la sécurité.

106 Soit le DSNA d'alors avait des difficultés avec la langue française, soit il s'agit d'une simple erreur typographique et il faut effectivement lire « absence de procédure miso ». Chacun jugera.

107 Depuis 2006, il y est écrit « évolution » ! Une procédure qui ne s'améliore pas, même avec l'amélioration continue.

108 Le terme « procédure MISO » est bien celui utilisé dans la PRO_002/DSNA et dans la MET_001/DSNA.

109 Répétition présente dans le texte original… depuis 2006 ! Quid de l'amélioration continue, moteur de la Qualité ?

110 Incidemment, le DSNA avait exigé « **que la programmation des opérations techniques pouvant affecter les moyens radio soit programmée dans les périodes de moindre trafic** » : ce qui ne signifie pas de les faire de nuit, sinon il aurait très bien pu l'écrire… Et « **en étroite concertation avec les services opérationnels** » : est-ce encore fait systématiquement aujourd'hui ? Rappelons juste qu'aujourd'hui RENAR-IP impacte la radio…

AVERTISSEMENT

Il est important d'insister sur le fait que, ces rappels concernant nos obligations et l'organisation de la DSNA, sont bien des rappels : sur un système dont nous pouvons par ailleurs critiquer certains aspects… Le but de ce dossier est de poursuivre notre connaissance du système de management de la DSNA à l'occasion de cette nouvelle version (très surprenante) du guide MISO : puisque, de fait, ceci n'est pas fait par l'administration, ou alors que très superficiellement[111]. Le problème pour nous n'est pas tant qu'un IESSA puisse parfois – à tort ou à raison – "dépasser la ligne", mais qu'il ait concrètement les moyens de savoir quand il la dépasse (« *un homme averti en vaut deux* »…).

En n'imposant plus l'obligation de procéder à une évaluation et à une atténuation des risques avant des interventions sur les équipements et les systèmes qui contribuent à la sécurité des vols, dont l'ensemble de la littérature consacrée à la maintenance s'accorde pour affirmer qu'elles figurent parmi les plus dangereuses, le directeur des opérations prend sa part de responsabilité : ce que nous ne pouvons que saluer.

Rappelons un autre exemple d'application des exigences de sécurité du « ciel unique européen » concernant spécifiquement les aides radio à la navigation, ainsi que trois articles fondamentaux pour les fonctionnaires (aussi bien pour nos autorités hiérarchiques que leurs subordonnés) :

> **Arrêté du 10 avril 2015 relatif à la mise en service et au suivi des aides radio à la navigation :**
>
> L'annexe au présent arrêté fixe les conditions de **MISE EN SERVICE**, d'**EXPLOITATION** et de **MAINTENANCE** des aides radio à la navigation …
>
> ANNEXE / **Exigences en matière de sécurité**
>
> Le prestataire de services de navigation veille à ce que l'**identification des dangers** ainsi que **l'évaluation et l'atténuation des risques** pour tous les changements relatifs aux systèmes ILS, VOR, NDB et DME **SOIENT SYSTÉMATIQUEMENT EFFECTUÉES**, conformément au règlement (UE) n° 1035/2011 du 17 octobre 2011.
>
> L'introduction d'un nouveau système et toute modification d'un système existant, **QUE CETTE MODIFICATION SOIT VOULUE OU SUBIE**, sont considérées comme des changements.
>
> **Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires (article 28) :**
>
> Tout fonctionnaire, quel que soit son rang dans la hiérarchie, est responsable de l'exécution des tâches qui lui sont confiées. Il doit se conformer aux instructions de son supérieur hiérarchique, **SAUF DANS LE CAS OÙ L'ORDRE DONNÉ EST MANIFESTEMENT ILLÉGAL ET DE NATURE À COMPROMETTRE GRAVEMENT UN INTÉRÊT PUBLIC**.
>
> Il n'est dégagé d'aucune des responsabilités qui lui incombent par la responsabilité propre de ses subordonnés.
>
> **Code pénal (article 122-4, alinéa 2) :**
>
> N'est pas pénalement responsable la personne qui accomplit un acte commandé par l'autorité légitime, **SAUF SI CET ACTE EST MANIFESTEMENT ILLÉGAL**.
>
> **Code pénal (article 432-1) :**
>
> Le fait, par une personne dépositaire de l'autorité publique, agissant dans l'exercice de ses fonctions, de **PRENDRE DES MESURES DESTINÉES À FAIRE ÉCHEC À L'EXÉCUTION DE LA LOI** est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Agissons en connaissance de cause.

111Pour des raisons que nous laissons le soin à chacun d'imaginer.

TABLE DES MATIÈRES