IESSA
au coeur

CONSTRUIRE
#2

SNIESSA
Syndicat National des IESSA

ÉLECTIONS 3-10 DÉCEMBRE 2026

“Les ingénieurs titulaires représentent à la fois des garanties sur le temps long de la maîtrise technologique des politiques menées par la puissance publique et une ressource sûre pour la relève des fonctions dirigeantes de l’État à forte composante technique”

Mission gouvernementale sur la haute fonction publique.
Rapport Guillou-Berger-Lavenir 2022



“La conception et le développement des systèmes d’IA à haut risque permettent, notamment au moyen d’interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant leur période d’utilisation.” - AI Act 2024/1689 chap III article 14 : l’UE impose une supervision de l’IA dans les systèmes critiques.

Construire #2

Table des Matières

Remettre les **IESSA au coeur** de la modernisation

Introduction 4
Un accord IESSA pour construire

Garantir la pérennité du corps 6
L'indispensable renforcement des capacités de l'ENAC

Intégrer les nouveaux enjeux 8
Vers une AE cyber et une prise en compte de l'IA

Moderniser en gardant le contrôle 10
Interview d'Uwe Schindler sur le modèle datacenter à la DFS

Effectifs IESSA et tendances 11
Cartographie des effectifs 2026

Introduction

Un accord IESSA pour construire

Dans notre premier numéro, nous avons posé les fondations : défendre notre périmètre, notre statut, nos droits. Protéger est indispensable, mais ne suffit pas. Un corps qui se contente de défendre ses acquis finit par péricliter. Il faut maintenant construire.

Les chiffres sont sans appel. En moins de dix ans, le nombre d'IESSA titulaires d'une AE est passé de 1 000 à 750, et plus de 380 de nos collègues partiront à la retraite d'ici 2035. Dans le même temps, la DSNA prévoit d'investir 850 M€ pour moderniser l'ATM. Ce plan ne peut aboutir sans ceux qui installent et maintiennent ces systèmes au quotidien. C'est pourquoi il faut recruter et former des IESSA en nombre.

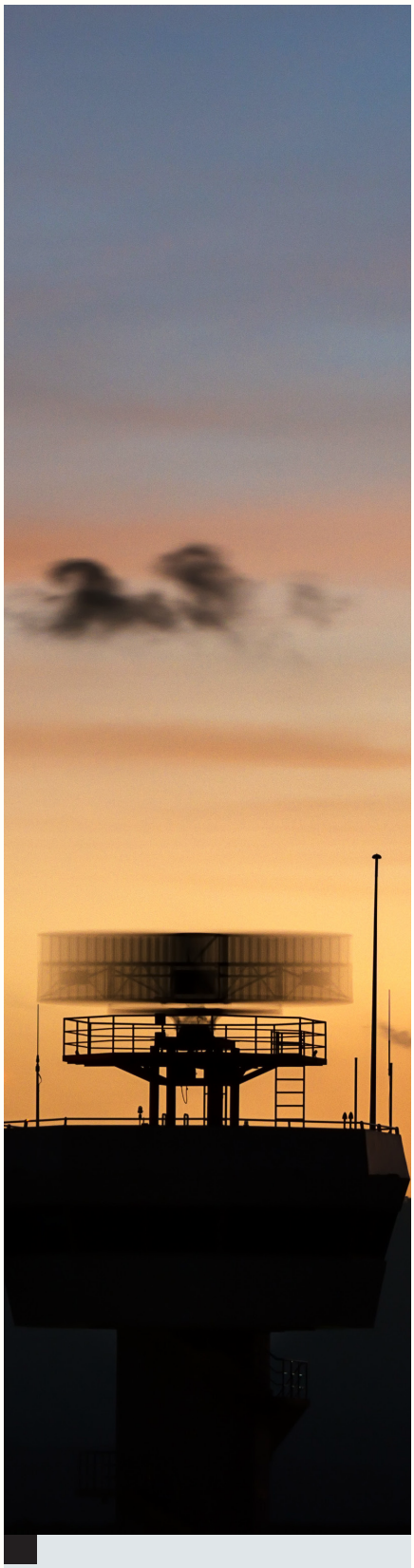
Nous avons besoin d'une ENAC forte, à deux promotions de 40 IESSA par an, dotée des moyens humains et matériels pour réussir. La formation initiale et continue doit intégrer l'intelligence artificielle et la cybersécurité, avec la création d'une AE cyber. La DSNA a fait le choix d'externaliser une partie de ces enjeux. Pour nous, il est essentiel de remettre les IESSA au cœur de la modernisation. C'est le sens de l'accord IESSA que nous porterons.

Objectifs clés

- Retrouver 1 000 IESSA détenteurs d'une AE.
- Ouvrir deux promotions de 40 IESSA par an.
- Reconnaître la charge de formation dans le calcul des effectifs.
- Créer une AE cyber.
- Garantir une IA maîtrisée par les IESSA.



IESSA au coeur de la DSNA et de la fonction publique.



Modernisation maîtrisée

La modernisation ne réussira qu'avec des effectifs qualifiés sur l'ensemble du système d'information d'importance vitale.

Accord IESSA

Les objectifs d'un accord
Construire

Le SNIESSA souhaite rassembler la profession autour d'un projet qui garantisse son avenir et celui du service public de navigation aérienne.

Effectifs

Augmenter la capacité de l'ENAC pour permettre de recruter deux promotions de 40 IESSA par an.

Modernisation

Rétablir nos capacités opérationnelles, avec un objectif de 1 000 IESSA détenteurs d'une AE.

Formation

Qualifier les IESSA en cybersécurité par la mise en place d'une AE dédiée, et lancer un plan d'adoption des technologies d'IA.

Sécurité

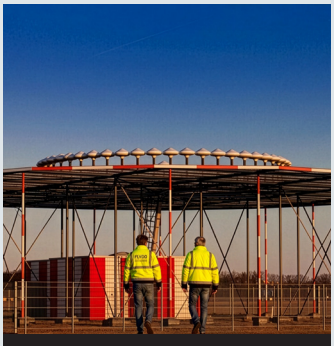
Garder le contrôle de nos systèmes en intégrant les nouvelles technologies dans le périmètre de la licence.





Soutenir la formation continue

L'augmentation des recrutements implique une mobilisation de tous les sites pour organiser les parcours de formation (PFE, QT, QTS) et qualifier sur les systèmes.
En 5 ans, ce sont presque 300 IESSA qui sont concernés. Il est nécessaire que cet effort soit accompagné et reconnu en incluant la charge de formation dans le calcul des effectifs.
Les premiers acteurs doivent être encouragés, en revalorisant notamment le poste d'instructeur licence et d'instructeurs ATSEP.
Le statut des stagiaires a lui aussi besoin d'évoluer. Dès leur arrivée, ils sont intégrés dans les activités de leurs sections et suivent le rythme de leurs collègues pour se qualifier sur les systèmes. Dès lors, il est légitime que leur régime horaire et leurs conditions de missions soient alignés.



Statut du stagiaire – aider l'intégration sur site.

Objectif 1000 AE

Beaucoup de littérature a été écrite pour expliquer les retards de la modernisation. Des rapports externes ont mis en avant des difficultés de gestion ou des erreurs stratégiques, et la DSNA a pointé du doigt une infrastructure technique trop complexe.
Les origines sont probablement multiples, mais une raison évidente a été écartée : le nombre d'IESSA titulaires d'une autorisation d'exercice. Ceux qui installent concrètement les systèmes et les maintiennent au quotidien sont naturellement un facteur de la réussite et du rythme des déploiements.

Le nombre d'autorisations d'exercice a chuté brutalement ces dernières années. En moins de 10 ans, le nombre d'IESSA avec AE est passé de 1000 à 750 ! C'est bien au-delà de la baisse des effectifs.

Ce phénomène se ressent pleinement dans les services techniques où la charge de travail moyenne augmente drastiquement, avec pour effet une dégradation des conditions de travail : pression sur les plannings, contraintes sur les congés et les formations, diminution du temps imparti à la rédaction de la documentation au sens large (opérationnelle, formation, MISO, études de sécurité…).

Bien sûr, les services techniques ne sont pas les seules victimes : la DTI a vu ses effectifs baisser de presque 8 % depuis 2020. L'appel à des prestations externes, sans cesse renouvelées, ne saurait être une solution efficace. La prise en compte du besoin passe par une connaissance de notre environnement, de nos méthodes de travail et de nos contraintes en termes de sécurité et de sûreté.

C'est le résultat d'une politique de l'administration, qui a cherché des marges de gestion dans les effectifs opérationnels et réorienté des postes vers la gestion de projets avec l'impression de faire un gain en ETP en les basculant d'un régime "horaires programmés" vers un régime "horaires de bureau". Ce calcul était une erreur fondamentale. Les ressources qui nous manquent pour déployer les systèmes n'ont pas été la priorité.

L'administration a donc elle-même créé une pénurie dans ses services techniques et à la DTI en privilégiant d'autres domaines. Ce choix complique considérablement les plannings de déploiement et fait peser de fortes contraintes sur les opérationnels. La priorité aujourd'hui est donc de rétablir nos capacités de maintenance et d'installation.

Le SNIESSA revendique le rétablissement des effectifs à 1000 IESSA détenteurs d'AE.

Garantir la pérennité du corps

Renforcer l'ENAC

Pour faire aboutir son plan de modernisation, la DSNA prévoit 850 M€ d'investissement ne serait-ce que pour le domaine ATM dans les prochaines années. En ajoutant les ressources qui seront nécessaires pour renforcer la résilience de nos infrastructures face à de nouvelles menaces, le plan de charge des services techniques va exploser. Une nécessité s'impose : qualifier et recruter pour augmenter les effectifs nécessaires à la modernisation.

Recrutement

Le concours BAC+2 doit être renforcé avec la mise en œuvre d'une deuxième promotion portant les capacités de formation à 2 fois 40 par année.

Cette organisation, calée sur les campagnes de mobilité, permettra de mieux gérer les mutations et les effectifs locaux.

Moyens

Nos collègues enseignants à l'ENAC doivent être soutenus dans leurs efforts pour construire une formation statutaire de qualité.

La DGAC doit investir dans les moyens humains et matériels de l'ENAC pour la formation IESSA.

Qualifications

Les évolutions des technologies et de nos missions appellent de nouvelles compétences.

La cybersécurité, la maitrise du cloud ou des systèmes IA ont vocation à être intégrées dans le cursus de formation initiale.

Tous les élèves, quel que soit leur cursus d'origine, doivent passer par l'ENAC et y suivre l'intégralité de leur formation. C'est ce socle commun qui leur permet d'arriver en affectation dans de bonnes conditions, dans le respect de la licence IESSA, avec l'ensemble des qualifications de domaine, puis d'obtenir les autorisations d'exercice.

Cet objectif est exigeant et devra continuer d'évoluer avec le contexte réglementaire et opérationnel. Dès lors, il faut que les moyens (stages en immersion, plateformes de TP, intervenants) soient mis en place pour former des ingénieurs de haut niveau avec des compétences en anglais, en cybersécurité et dans le domaine de l'IA.

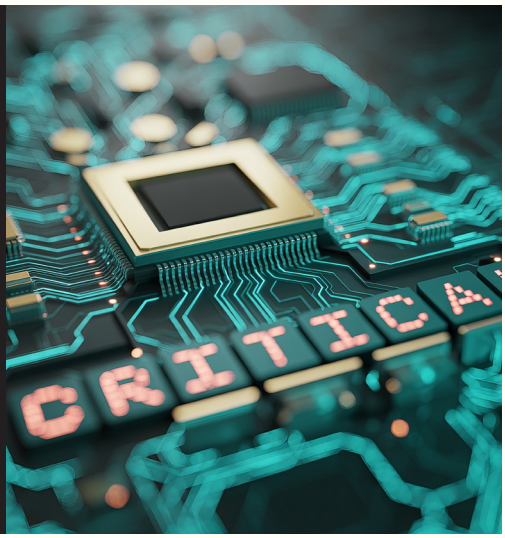
La coopération entre les sites et l'ENAC est, elle aussi, primordiale pour réussir le parcours de qualification. C'est une école d'application qui prépare directement à l'exercice d'un métier qui s'enrichit de l'expérience du monde opérationnel. Toutes les initiatives qui permettent de faire travailler ensemble les collègues en école et dans les centres doivent être encouragées et facilitées par la DSNA.



L'ENAC est une école d'application et donc un fondement du statut IESSA comme pour tous les corps d'État.

IA
de confiance

Intégration de l'IA dans les systèmes critiques
L'IA doit être comprise et contrôlée pour espérer une adoption et une certification***.



***À lire : règlement (UE) 2024/1689 Annexe III - IA dans les systèmes à haut risque.

Plan d'adoption IA

La DSNA doit anticiper l'arrivée de l'IA dans le monde ATM et préparer un plan de transformation pour que nos services maîtrisent cette technologie.

Le premier enjeu est la protection de nos données. Elle passera par des modèles internes, qui devront être maintenus par des IESSA sur des infrastructures propres. Vient ensuite la maîtrise technologique : nous devons garder le contrôle des systèmes opérationnels qui intégreraient tout ou partie d'IA.

L'IA n'est pas qu'un effet de mode. Elle peut rendre les services plus efficaces, par exemple pour produire de la documentation ou rédiger des procédures. Nous devons savoir nous en servir, et c'est devenu indispensable pour toute activité technologique moderne. D'autres domaines similaires au nôtre, comme le nucléaire, ont déjà intégré leur IA maison pour gérer leur système de documentation.

Reste l'usage de l'IA sur les systèmes critiques, qui renvoie à la notion d'IA de confiance. Pour être acceptée dans un environnement critique, elle doit être transparente, comprise et donc supervisée. Les IESSA doivent être les garants du fonctionnement de ces systèmes.

Les travaux sur la réglementation de l'IA dans les infrastructures critiques sont déjà engagés dans l "AI Act" européen. Il confirme la nécessité d'avoir une supervision humaine de ces applications pendant qu'elles sont en utilisation (chap. III, art. 14). Sans cette maîtrise interne et indépendante qui permet d'expliquer et de prévoir les comportements des systèmes d'IA, il serait illusoire d'espérer une certification pour des applications dans le domaine opérationnel.

Cette évolution doit être anticipée dès maintenant. Le SNIESSA appelle à un plan de formation sur ces technologies, à la prise en main d'outils basés sur l'IA par la DTI et les services techniques, et à l'implication d'experts opérationnels dans la conception d'une doctrine interne d'usage.

- Utiliser des modèles internes pour protéger nos données.
- Construire une compétence dans les ST et à la DTI pour garder la maîtrise.
- Superviser pour permettre l'intégration en environnement critique.
- Se préparer aux contraintes réglementaires de certification.

Intégrer les nouveaux enjeux

La DSNA est le premier ANSP d'Europe. Autrefois leader technologique de l'ATM, elle peine aujourd'hui à se moderniser. Afin de ne pas commettre les mêmes erreurs, il est de l'intérêt de tous que l'on se prépare à intégrer les évolutions technologiques dans un contexte où la maîtrise interne devient un impératif. Il y a d'abord une urgence à mieux prendre en compte la cybersécurité dans nos missions, et ensuite à se préparer à l'arrivée de l'IA, qui sera aussi destinée à des applications critiques.

Qualification en cybersécurité



Vers une AE cyber

Le contexte international se prête particulièrement à une réflexion sur la capacité de la DSNA, grâce à ses IESSA, à prévenir les attaques cyber et surtout à y remédier. Le thème de la résilience est devenu grand public et les autorités comme les usagers attendent tous du service public de navigation aérienne qu'il se protège et se prépare.

Au plus près des systèmes, nous ne pouvons avoir qu'une vision lucide sur notre organisation et le manque d'implication des opérationnels et de la DTI dans le domaine de la cybersécurité.

En dépit de notre expertise sur les systèmes et les architectures, notre administration a fait le choix d'écarter systématiquement les IESSA des enjeux cyber. En externalisant ces services, elle s'est privée d'une capacité à réagir vite, alors que la sécurité, la sûreté et la défense nationale sont en jeu et que les attaques peuvent survenir à tout moment, de jour comme de nuit, toute l'année.

Les raisons qui ont conduit à ces choix n'ont rien de rationnel et ne sont pas à la hauteur des enjeux. Le SNIESSA juge indispensable de réinternaliser l'ensemble de la cyberdéfense.

Ce besoin doit se traduire dans la formation des IESSA et dans la vérification de leurs compétences, afin de garantir qu'ils sauront traiter l'ensemble des incidents de cyberdéfense. Une brique "Cybersécurité" dans nos autorisations d'exercice est le moyen qui permettra d'y répondre.

Cette AE cyber permettra de bâtir des cursus de formation initiale, de formation continue et de vérification des compétences. Les IESSA seront ainsi entraînés régulièrement à répondre à ces incidents, et la DSNA, en tant que prestataire de navigation aérienne, conservera un haut niveau de sécurité, de sûreté et de défense nationale.

Enfin, le SNIESSA restera particulièrement attentif à ce que nos activités soient réellement conformes aux réglementations qui s'appliquent dans ce domaine et que nos collègues, en première ligne, ne soient pas exposés à des risques juridiques.



> À la DFS l'infrastructure cloud est dans le domaine de compétence des ATSEP.

Moderniser
en gardant le contrôle

Infrastructure cloud l'exemple allemand

Interview de Uwe Schindler, ATSEP à la DFS et membre de la FSTD (Flugsicherungstechnik), la branche ATSEP de GdF. Spécialiste ATM, il travaille depuis de nombreuses années sur les questions de qualification ATSEP, de cloud et d'évolution des architectures ATM.

Comment la DFS a-t-elle abordé l'arrivée du cloud dans l'ATM ?

Il y a d'abord eu un accord social sur le périmètre et les responsabilités des ATSEP. Le datacenter et le cloud ont été intégrés à leurs tâches. Aujourd'hui, la plateforme cloud et les services utilisés pour l'ATM sont donc exploités par des ATSEP spécifiquement qualifiés. Le cloud n'est donc pas une simple infrastructure IT : c'est un composant critique du système fonctionnel ATM. À ce titre, il a été intégré à notre système de licence.

Comment avez-vous construit cette nouvelle compétence ?

Des ATSEP ont été formés et qualifiés aux compétences cloud et des spécialistes du cloud sont venus apporter leur expertise. Certains d'entre eux ont même été recrutés puis ont suivi le cursus de formation initiale et sont devenus ATSEP. Pour être plus précis sur les compétences, on parle ici de virtualisation, de réseaux, d'hyperviseurs, de VMware, de Red Hat OpenShift ou encore d'architectures SOA. L'important est de garder une vision suffisamment large du système.

Pourquoi est-ce important de garder ces compétences en interne ?

En cas de problème, il faut pouvoir comprendre ce qui se passe et agir, et donc connaître intimement les réseaux, la virtualisation, les plateformes et leurs interactions. Maintenir cette compétence en interne a un coût, notamment RH, mais c'est indispensable pour conserver la maîtrise du système, être plus réactif et autonome, et surtout renforcer sa résilience.

DFS

Deutsche Flugsicherung

Prestataire allemand de services de navigation aérienne.

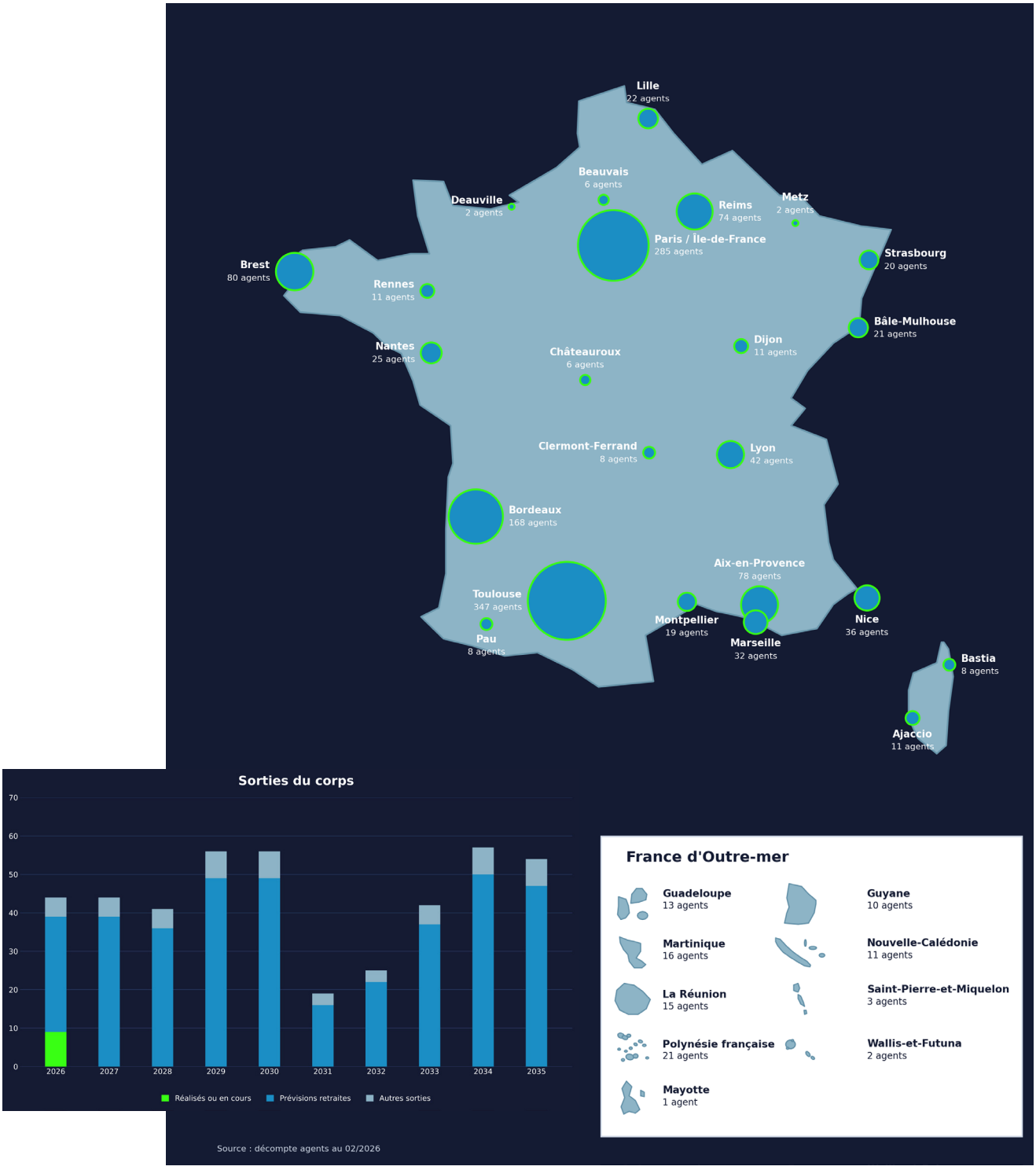
GdF

Gewerkschaft der Flugsicherung

Syndicat professionnel de référence à la DFS, fortement implanté parmi les personnels opérationnels.

Effectifs & tendances

La pyramide des âges de notre corps est telle que, d'ici 2035, plus de 380 collègues partiront à la retraite (25 % du corps). Le SNIESSA revendique le passage à 2 promotions de 40 IESSA par an afin d'inverser la tendance et de retrouver les effectifs compatibles avec les enjeux auxquels nous faisons face. Il faudra , dans le même temps, renforcer les équipes formation de l'ENAC tant en moyens humains qu'en moyens matériels.



SNIESSA - CONSTRUIRE
ÉLECTIONS 3 AU 10 DÉCEMBRE 2026
BN@IESSA.ORG