

 Fédération Nationale de l'Aviation et de ses Métiers	Commission Affaires Techniques et Réglementaires
Date : 14/03/2024	Compte-rendu

Participants

- Anaïs BENSÂÏ – GEH
- Olivier SCIARA – UAF
- Alexandre DI CIOCCIO – LA COMPAGNIE
- Carinne HEINEN – EASY JET
- Fabrice BENERO – AIR FRANCE
- Alain CORBEL - HOP
- Marc-Antoine BLONDEAU – FRENCH BEE
- Richard VERON – AIR FRANCE
- Christophe COTTREZ – HOP
- Isra BENDJEMA – CORSAIR
- Alison RIBOUT – TIME TO FLY
- Stéphanie MACQUET – JCP CONSEIL
- Fayçal BERREHILI – DASSAULT FALCON SERVICES
- Christophe ROSSET – SNEH
- Claire DUPIRE - FNAM
- Diane BERTONCINI – FNAM
- Cyril BEUCHET – FNAM
- Muriel ASSOULINE – AIR CARAIBES ATLANTIQUE
- Julian MARTINELLI - TRANSAVIA
- Renaud LEPELIER – AIR France
- Olivier OUTTIER - DSAC

Ordre du jour

1. Point réglementaire

- a. Présentation par Olivier Outtier (DSAC) sur le rôle et les travaux du pôle Coopération Européenne et Réglementation de Sécurité
- b. Opinion 01-2024: Ground Handling Requirement
- c. NPA 2023-10: Part-147
- d. Workshop EASA: Fatigue Risk Management (FRM)

2. Point sur les groupes de travail & comités

- a. Cybersécurité
 - i. Groupe de travail
 - ii. Part-IS - Part IS allégée
 - iii. Exercice de Coordination de Crise du CCTA
 - iv. CERT Aviation France
 - v. AirCyber de BoostAerospace
- b. Comité CSCE
- c. CSCA
- d. GT Maintenance GIPAG/ SNEH

 Fédération Nationale de l'Aviation et de ses Métiers	Commission Affaires Techniques et Réglementaires
Date : 14/03/2024	Compte-rendu

3. Sujets en cours

- a. DSNA: Implémentation de 4-Flight
- b. Mesures JO:
 - i. Retour sur les COMEX de Coordination des Aéroports
 - ii. Mesures de sûreté

4. Points divers et problématiques

- a. Point divers
- b. Séance d'échange et tour de table

1. Point réglementaire

a) Présentation par Olivier Outtier (DSAC) sur le rôle et les travaux du pôle Coopération Européenne et Réglementation de Sécurité

Voir la présentation.

Précisions à propos de la présentation :

- Les règlements EASA sont constitués d'actes d'exécution et d'actes délégués. Les actes d'exécution sont soumis au vote des états membres, tandis que les actes délégués peuvent être adoptés directement par l'EASA (on retrouve le règlement FTL ainsi les règlements issus de l'OACI). Les modalités sont décrites dans le règlement de base (UE) 2018/113.
- Le pôle DSAC ERS est impliqué sur les sujets d'actualité suivants : FTL hélicoptères et aviation d'affaires, la NPA 2023-10 Part 147, l'opinion 2024-01 relatif à l'assistance en escale, l'eMCO...

Les participants ont rappelé qu'il y a une complication des règlements post-covid (LVO, Fuel Management, CBT...).

b) Opinion 01-2024: Ground Handling Requirement

Pas de remarques.

Voir la présentation.

c) NPA 2023-10: Part-147

Voir la présentation.

Voici les principales remarques présentées à l'EASA :

- Le système de gestion n'est pas aligné sur les autres règlements ;
- Il faudrait compléter la formation L66 avec un module ou un examen d'anglais qui validerait la licence.
- Il faudrait laisser la possibilité pour les organismes Part 147 d'organiser eux-mêmes l'examen ou le module d'anglais

 Fédération Nationale de l'Aviation et de ses Métiers	Commission Affaires Techniques et Réglementaires
Date : 14/03/2024	Compte-rendu

d) Workshop EASA: Fatigue Risk Management (FRM)

Voir la présentation.

La différence entre le FRM & FRMS est difficile à appréhender par les organismes (c'est également le cas pour études scientifiques à mettre en place dans la cadre du FRMS).

Rappel :

Le FRM est le concept plus large qui englobe la philosophie et les stratégies pour gérer les risques liés à la fatigue, tandis que le FRMS est la mise en œuvre spécifique du FRM au sein d'une organisation à travers un système structuré de processus et de mesures.

2. Point sur les groupes de travail et comités

a) Cybersécurité

- Groupe de travail

Pas de remarques.

- Part-IS - Part IS allégée

Pas de remarques.

- Exercice de Coordination de Crise du CCTA

Il est recommandé si possible de réaliser un exercice de crise cyber avant les JO.

- CERT Aviation France

Pas de remarques.

- AirCyber de BoostAerospace

Une présentation D'AirCyber va être organisée par la FNAM en partenariat avec le CERT Aviation France.

- Autre : Formation Cybersécurité des pilotes : étude ASL

Vous trouverez en annexe l'étude complète.

L'étude Cyber a été conjointement menée par la DGAC, l'Aviation Civile Israélienne, et ASL Airlines qui fournit les équipages.

L'objectif est d'évaluer l'efficacité et les besoins en formation cybersécurité pour les pilotes, et leur capacité à réagir efficacement à des attaques cyber en vol.

 Fédération Nationale de l'Aviation et de ses Métiers	Commission Affaires Techniques et Réglementaires
Date : 14/03/2024	Compte-rendu

Contexte :

- 16 équipages répartis en 2 groupes de 8 équipages : un groupe suit un module d'e-learning sur les menaces cyber juste avant la séance d'entraînement au simulateur, l'autre non.
- Expérience réalisée sur simulateur, durant une séance standard.
- Aucun équipage n'est prévenu qu'il va recevoir 5 attaques cyber distinctes.

Scénarios :

	Attaques spoofing simulées	Réaction - Groupe formé cyber	Réaction - Groupe Sans formation cyber
#1	Un signal ADS-B factice est diffusé au contrôleur aérien, créant une confusion sur l'altitude réelle de l'avion	Les équipages ont eu tendance à croire l'ATC, mais ont cherché à lever le doute	Idem
#2	En croisière, réception d'un faux message ACARS indiquant un ZFW erroné (5T de moins)	Vérification par ACARS auprès des OPS	Idem
#3	Spoofing des données de consommation de carburant : la qté de fuel est maintenue voire augmentée malgré remise de gaz	Non perçu par les équipages, aucune action entreprise	Idem
#4	Pendant une approche RNAV, le GPS est faussé à un taux lent mais constant, amenant l'avion à s'écarter de sa trajectoire de vol prévue	Reconnaissance précoce des écarts et ajustement de la trajectoire	Idem
#5	Fausse alerte EGPWS	Reconnaissance d'une fausse alarme liée au bon contact visuel avec la piste. Application systématique des SOP.	Idem

Conclusions :

1. Méconnaissance des pilotes au sujet des attaques cyber : aucun des équipages n'a identifié qu'il avait subi des attaques cyber, et que ce type d'attaques pouvaient survenir lors d'un vol régulier commercial ;
2. E-learning inefficace
3. La sécurité n'a jamais été compromise
4. **L'expérience de subir les cyberattaques au simulateur a été bien plus efficace que le e-learning.** À la suite du débriefing, les deux tiers ont conclu qu'ils étaient désormais bien plus conscients du risque et des effets sur la sécurité des vols, et 90% sont convaincus de l'importance du reporting cyber.

 Fédération Nationale de l'Aviation et de ses Métiers	Commission Affaires Techniques et Réglementaires
Date : 14/03/2024	Compte-rendu

b) Comité CSCE

Pas de remarques.

c) CSCA

Pas de remarques.

d) GT maintenance GIPAG / SNEH - OSAC

En amont du prochain GCCCTA OSAC, un mail a été envoyé par la FNAM à la direction d'OSAC, listant l'ensemble des incohérences que nous avons relevées durant la phase de dépôt des MOE.

Nous avons également suggéré à OSAC de partager les rapports d'audit entre les responsables de surveillance à l'issue de chaque audit, pour une meilleure standardisation.

De plus, nous avons également mentionné la problématique du dernier audit OSAC d'Air Caraïbes Atlantique.

Nous reviendrons vers vous après réception de la réponse d'OSAC.

La réunion de la section « surveillance et certification »- activités OSAC – de la commission consultative économique du budget annexe « Contrôle et exploitation aériens », aura lieu le 27 mars 2024.

3. Sujets en cours

a) DSNA: Implémentation de 4-Flight

Une réunion de débriefing des dernières UOP de 4-Flight aura lieu le 5 avril 2024. La DSNA présentera également à cette occasion, les mesures qui ont été décidées pour l'implémentation de 4-flight en novembre 2024.

b) Mesures JO:

- Retour sur les COMEX de Coordination des Aéroports

Pas de remarques.

- Mesures de sûreté

Pas de remarques.

 Fédération Nationale de l'Aviation et de ses Métiers	Commission Affaires Techniques et Réglementaires
Date : 14/03/2024	Compte-rendu

4. Points Divers et Problématiques

a) Points divers

- **EASA Safety Week:** Lien ici pour s'enregistrer ci-dessous
<https://easa-webmeetings.webex.com/webappng/sites/easa-webmeetings/webinar/webinarSeries/register/dedb613cbbd4427089f9e4a84cc0a734>
 - Day 1: 22/04/2024 – Introduction and Top Safety Issues: 10:00 - 11:30 CET (UTC +1)
 - Day 1: 22/04/2024 – Aerodromes and Ground Handling: 14:00 - 15:30 CET (UTC +1)
 - Day 2: 23/04/2024 – Air Operations 10:00 - 11:30 CET (UTC +1)
 - Day 2: 23/04/2024 – ATM/ANS: 14:00 - 15:30 CET (UTC +1)
 - Day 3: 24/04/2024 – ATO/ Flight Crew Training: 10:00 - 11:30 CET (UTC +1)
 - Day 3: 24/04/2024 – Continuing Airworthiness: 14:00 - 15:30 CET (UTC +1)
 - Day 4: 25/04/2024 – Cyber/ Security: 10:00 - 11:30 CET (UTC +1)
 - Day 4: 25/04/2024 – Safety Leadership: 14:00 - 15:30 CET (UTC +1)
- **Air France : TAXIBOTS**

Rappel : Le TaxiBot est un véhicule tracteur hybride semi-robotique conçu pour transporter des avions de la porte d'embarquement à la piste de décollage sans utiliser les réacteurs.

Une expérimentation a eu lieu à CDG avec Air France.

Voici un échantillon des conclusions :

- Il est difficile pour la DSNA de gérer ces nouveaux « types d'engins » en co-activité avec les autres engins, véhicules et aéronefs ;
 - Il n'apporte pas une réduction de coût significative ;
 - Introduire le taxibot, impliquerait des travaux importants au niveau de l'infrastructure aéroportuaire ;
 - La compagnie KLM a été obligée de le mettre en place à Schiphol. Il faut être vigilant pour que ces mesures ne s'étendent pas jusqu'à la France.
- **Dates des prochaines CAT&R :**
 - 27 juin 2024 ;
 - 07 novembre 2024 ;

*N'hésitez pas à revenir vers nous si vous avez des questions.
L'équipe de la FNAM.*



Fédération
Nationale de l'Aviation
et de ses Métiers

Affaires Techniques et Réglementaires

Commission #29 – 14 Mars 2024

Ce document ne saurait s'interpréter
sans les commentaires oraux qui
l'accompagnent

Ordre du jour

1^{ère} partie

Point réglementaire

- ❖ Présentation par Olivier Outtier (DSAC) sur le rôle et les travaux du pôle Coopération Européenne et Réglementation de Sécurité
- ❖ Opinion 01-2024: Ground Handling Requirement
- ❖ NPA 2023-10: Part-I47
- ❖ Workshop EASA: Fatigue Risk Management (FRM)

2^{ème} partie

Point sur les groupes de travail & comités

- ❖ Cybersécurité
 - ❖ Groupe de travail
 - ❖ Part-IS - Part IS allégée
 - ❖ Exercice de Coordination de Crise du CCTA
 - ❖ CERT Aviation France
 - ❖ AirCyber de BoostAerospace
- ❖ Comité CSCE
- ❖ CSCA
- ❖ GT Maintenance GIPAG/ SNEH

3^{ème} partie

Sujets en cours

- ❖ DSNA: Implémentation de 4-Flight
- ❖ Mesures JO:
 - ❖ Retour sur les COMEX de Coordination des Aéroports
 - ❖ Mesures de sûreté

4^{ème} partie

Points divers et problématiques

- ❖ Point divers
- ❖ Séance d'échange et tour de table



Rôle et travaux du pôle Coopération Européenne et Réglementation de Sécurité.

Point Réglementaire : *Opinion 01-2024 Ground Handling Requirement (1/2)*

Surveillance par l'autorité (ARGH.GEN.100 & ORGH.GEN.105):

Une seule déclaration doit être envoyée à l'autorité même si l'organisme a des bases établies dans plusieurs pays EASA (single GH organisation business grouping).

Afin de simplifier la surveillance des organismes dans les différents pays de l'UE, l'EASA propose un principe de « surveillance collaborative » entre les pays:

- Une base principale établie par l'organisme: Audit système de gestion & Audit « opérationnel » par l'autorité dans laquelle cette base est établie;
- Un audit focus « opérationnel » dans chacune des bases par l'autorité de chaque pays (comme SAFA)

Le planning de surveillance de 48 ou 72 mois est défini en fonction de la maturité du SMS de l'organisation.

Une base dans un pays tiers ne sera pas sous le scope EASA, mais sous la responsabilité du pays tiers dans laquelle la base est établie.

Surveillance par une compagnie aérienne

Les compagnies devront prendre en compte les résultats d'audits de l'autorité afin d'adapter la surveillance de ses sous-traitants. L'idée est de réduire le nombre d'audits, et la durée en se focalisant sur des sujets particuliers.

Système de gestion (ORGH.MGM.200)

SMS différencié en fonction de la taille et la complexité des opérations. Une organisation est considérée « small » jusqu'à 10 ETP (nombre d'ETP lissé sur l'année).

Point Réglementaire : *Opinion 01-2024 Ground Handling Requirement (2/2)*

ERP (Emergency Response Plan)

L'ERP qui était défini en IR (implementing rules), est devenu un GM (guidance material): la référence est GM3 ORGH.MGM.200(b)(2)

Safety manager (ORGH.MGM.210)

Un safety manager doit être défini. Il doit avoir un accès direct au DR. Il peut nommer des responsables/ coordinateurs sécurité sur chaque base, ou/et en fonction des départements de l'organisation. Il doit être formé selon l'AMC2 ORGH.MGM.210(b)(1).

Langue commune (ORGH.TRG.115)

L'organisation doit garantir une communication efficace au sein de l'organisation, ou avec le personnel de l'aérodrome, les équipages... Il n'y a pas de langue obligatoire. La langue commune doit être décidée par l'organisation GH, l'exploitant de l'aérodrome et l'exploitant de l'aéronef auquel les services sont fournis.

Information Security (Part-IS)

Une phase de transition de 6 ans (après l'entrée en vigueur du règlement) est proposée pour appliquer la Part-IS.

Critères d'applicabilités:

'(c) ground handling organisations subject to Regulation (EU) xx [ground handling] that:

1.(i) in order to provide the respective services, have to collect, store, analyse or otherwise process data provided by third parties; or

2.(ii) provide directly to aircraft operators data that will be used for operational purposes.';

Les critères ne sont pas assez précis. En cours de discussion avec la DGAC.

Point Réglementaire : *NPA 2023-10 Part-147 (commentaires envoyés le 29 février)*

Principaux changements:

- a) Introduction d'exigences en matière de:
 - *système de gestion* pour les 147 afin d'identifier clairement les lignes de responsabilités et les tâches au sein de l'organisation, ainsi que d'identifier et de définir les principaux processus à décrire par l'organisation ;
 - *qualification et de responsabilités du personnel de l'organisation*, y compris l'évaluation de la compétence et les exigences linguistiques, et modifications des exigences en matière de formation initiale et continue pour le personnel.
- b) Modifications des exigences:
 - relatives au processus de suivi de la conformité,
 - relatives aux procédures de formation,
 - pour le processus d'examen et la sécurité du matériel d'examen.
- c) Modifications des privilèges de l'organisation et introduction de limitations et de conditions concernant l'exercice de certains privilèges, par exemple un nombre limité d'activités de formation dans des lieux « non approuvés »
- d) Introduction de dispositions pour des moyens de conformité alternatifs.
- e) Modifications des exigences du MTOE pour inclure les changements mentionnés dans les points ci-dessus.
- f) Exigences pour des rapports d'activité (contenant des informations sur la prestation de formation et d'examens avec un accent particulier sur les résultats).
- g) Promotion d'accords pour la supervision des examens.

Point Réglementaire : *Workshop EASA, Fatigue Risk Management (FRM) (1/3)*

- I. Plusieurs présentations ont été faites par des compagnies aériennes au sujet du FRM:
 - les outils et process utilisés (en fonction des phases: proactives, prédictives et réactives);
 - Les formations dispensées (incluant les formations dispensées au personnel sol);

Ces présentations seront détaillées au prochain GT gestion de la fatigue qui se **déroulera le 02 avril à 14H30.**

2. Des clarifications sur le FRM+S (ORO.FTL.120) vont être développées prochainement dans une RMT (rules making task)

Point Réglementaire : *Workshop EASA, Fatigue Risk Management (FRM) (2/3)*

3. EASA ED/Decision 2023/023/R publiée en décembre 2023: <https://www.easa.europa.eu/en/document-library/agency-decisions/ed-decision-2023023r>

→ Le concept « **Appropriate FRM** » s'applique à l'ensemble des services de nuit, ainsi qu'aux services qui se terminent tard (auparavant il s'appliquait seulement aux services de nuit d'une durée supérieures à 10H)

Rappel « Late night duty » ou service qui se termine tard: une période de service se terminant entre 00h00 et 01h59 dans le fuseau horaire auquel un membre d'équipage est acclimaté;

Ajout de recommandations:

- Les services de nuit, d'une durée supérieure ou inférieure à 10 heures, sont associés à une probabilité accrue de niveaux élevés de fatigue au début de descente (TOP).
- Il y a une probabilité élevée que les niveaux de fatigue soient plus élevés au TOD durant des services non-consécutifs qui se terminent tard, et des services de nuit non-consécutifs.
- 3 sous-types de services de nuit sont distingués et classés par probabilités d'occurrence de niveaux de fatigue élevés au TOD: **(les opérateurs doivent appliquer des mesures différenciées selon la sous-catégorie de service de nuit CS FTL.1.205)**
 - FDP (flight duty period) qui débute entre 2.00 h et 4.59 h;
 - FDPs qui se terminent entre 2.00 h et 5.59 h, et qui débutent à 1.59 h ou plus tôt;
 - FDPs qui se terminent à 6.00 h ou plus tard et qui débutent à 1.59 h ou plus tôt.
- Les responsabilités partagées ont d'avantage été détaillées dans le GM3 CS.FTL.1.205(a)(2) pour les vols du scope « appropriate FRM »

Point Réglementaire : *Workshop EASA, Fatigue Risk Management (FRM) (3/3)*

3. EASA ED/Decision 2023/023/R publiée en décembre 2023: <https://www.easa.europa.eu/en/document-library/agency-decisions/ed-decision-2023023r>

Différence entre « Appropriate FRM » & FRM (ORO.FTL.I20)

« **Appropriate FRM** » est un terme choisi pour désigner un ensemble de principes et d'outils qui soutiennent l'opérateur et son personnel opérationnel dans la gestion de certains risques liés à la fatigue et des risques associés au travers du SGS, en restant en conformité avec les limites de temps de service, les limites de temps de vol et les exigences de repos définies par la sous-partie ORO.FTL.

Un système FRM selon l'article ORO.FTL.I20 est un complément fondé sur des données scientifiques à la réglementation, qui gère la fatigue de l'équipage de manière flexible en tenant compte de l'exposition au risque et de la nature des opérations. Les opérateurs ont besoin d'un tel système FRM lorsqu'ils s'écartent des spécifications de certification ou lorsqu'ils appliquent un mélange de règles prescriptives et d'arrangements flexibles.

Inversement, le concept de « appropriate FRM » soutient la mise en œuvre des règles et est appliqué sans s'en écarter.

Ordre du jour

1^{ère} partie

Point réglementaire

- ❖ Présentation par Olivier Outtier (DSAC) sur le rôle et les travaux du pôle Coopération Européenne et Réglementation de Sécurité
- ❖ Opinion 01-2024: Ground Handling Requirement
- ❖ NPA 2023-10: Part-I47
- ❖ Workshop EASA: Fatigue Risk Management (FRM)

2^{ème} partie

Point sur les groupes de travail & comités

- ❖ Cybersécurité
 - ❖ Groupe de travail
 - ❖ Part-IS - Part IS allégée
 - ❖ Exercice de Coordination de Crise du CCTA
 - ❖ CERT Aviation France
 - ❖ AirCyber de BoostAerospace
- ❖ Comité CSCE
- ❖ CSCA
- ❖ GT Maintenance GIPAG/ SNEH

3^{ème} partie

Sujets en cours

- ❖ DSNA: Implémentation de 4-Flight
- ❖ Mesures JO:
 - ❖ Retour sur les COMEX de Coordination des Aéroports
 - ❖ Mesures de sûreté

4^{ème} partie

Points divers et problématiques

- ❖ Point divers
- ❖ Séance d'échange et tour de table

Points sur les groupes de travail & comités : *Cybersécurité (1/5)*

Groupe de travail

Mise en conformité avec le guide DGAC 3CF et préparation à la mise en conformité avec la Part IS

- 15 sessions déjà réalisées (*participants réguliers: Chailair/ Corsair/ FrenchBee & ACA/ HOP/ La Compagnie/ Transavia/ ATI*)
- Prochaine session le 28/03/2024
- *Objectifs du GT*
 - ❖ *Identification des évènements redoutés, avec la gravité associée*
 - ❖ *Associer les sources de risques et les objectifs visés, avec identification des motivations, ressources et activité pour chaque compagnie*
 - ❖ *Construire la cartographie de menace numérique de l'écosystème et sélectionner les parties prenantes critiques*
 - ❖ *Construire les scénarios opérationnels (modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques)*

Derniers travaux:

- Etude de la consultation NIS v2 (30/11/23)
- Etude de risques des systèmes de communications (20/02/24 – non terminée)

Prochains travaux:

- Etude de risques des systèmes de navigation et des systèmes de surveillance

Points sur les groupes de travail & comités : *Cybersécurité (2/5)*

Part-IS allégée: applicable aux “petites” organisations avec impact cyber sur la sécurité aérienne limité et acceptable

Utilisation de la clause Part-IS de PROPORTIONALITE [IS.I.OR.200(d)] → **Exigences cyber adaptées aux « petits »**
Alternative moins contraignante, mais **cohérente avec les objectifs de la Part IS**

Création d'une étude d'impacts sur le risque cyber par la FNAM, permettant de définir un profil de risque en termes de cybersécurité pour l'ensemble des organisations soumises aux règlements suivants :

- (EU) No 965/2012 (CAT, SPO, NCC)
- Regulation (EU) No 1321/2014 (I45, CAMO)
- Regulation (EU) No 1178/2011 (ATO, FSTD)
- Opinion 01/2024 (à venir ...)

L'échelle a été définie entre 0 et 10.

Ce projet, soutenu par la DSAC pôle « Cybersécurité » a été présenté à Patrick Cipriani (Directeur de la DSAC) le 28 février dernier en considérant dans un premier temps le règlement N°965/2012.

Prochaines étapes:

- Validation de plusieurs paramètres avec DSAC-NO (navigabilité et opérations);
- Etendre l'étude aux I45, CAMO, ATO, FSTD
- Etendre à l'assistance en escale

Points sur les groupes de travail & comités : *Cybersécurité (3/5)*

Exercice de Coordination de Crise du CCTA

- Exercice préparé par deux personnels de la DSNA et du CERT Aviation France. Les participants et observateurs ont été briefés lors de deux séances dédiées précédant l'exercice.
 - Malgré l'épisode neigeux dans le nord de la France, l'exercice s'est déroulé comme prévu. La trame générale du scénario a pu être déroulée de façon nominale dans le respect du timing visé.
 - Le pack d'entraînement pour les Jeux Olympiques et Paralympiques mis en ligne par l'ANSSI a été partiellement utilisé. Voici le lien: <https://cyber.gouv.fr/actualites/jop-2024-lanssi-met-disposition-un-kit-dexercice-jop-massifie>
- Il est vivement conseillé de réaliser un exercice de crise cyber en interne avant les JO. Pour le moment, une seule compagnie a prévu d'en faire un.**
- Les prochains exercices de crise cyber seront organisés dans le cadre du CERT Aviation France. N'hésitez pas revenir vers nous si vous souhaitez y participer (date non communiquée pour le moment).

Points sur les groupes de travail & comités : *Cybersécurité (4/5)*

CERT Aviation France

Le CERT (*computer emergency response team*) Aviation fournit les services suivants :

- Réponse aux incidents de premier niveau (actions réflexes techniques et réglementaires, coordination avec les autorités françaises et le CSIRT régional),
- Veille sur les vulnérabilités,
- Sensibilisation des bénéficiaires.

Le CERT Aviation France est composé de membres fondateurs et de membres. Les membres fondateurs sont Air France, le groupe ADP, Dassault Aviation, la DGAC, la FNAM, Thalès AVS, et l'UAF. Toute organisation du secteur de l'aviation peut adhérer à l'association.

Tous les adhérents de la FNAM (CSTA, EBAA, GIPAG, GPMA, SNEH, CSAE) peuvent désormais bénéficier gratuitement des services de base du CERT Aviation.

Le service de réponse à incident cybersécurité du CSIRT Aviation est désormais opérationnel et disponible.

Les membres de la FNAM peuvent composer le 01 81 70 71 72 ou écrire à assistance@cert-aviation.fr.

Un analyste vous aidera à :

- Qualifier l'incident et appliquer les actions réflexes s'il s'agit bien d'un incident cyber,
- Effectuer les déclarations réglementaires auprès des organismes de tutelles et régulateurs (CNIL, ANSSI)
- Mobiliser les services de l'Etat pour le dépôt de plainte si vous le souhaitez.

Ce service est disponible 24H/24 et 7J/7.

Le CSIRT Aviation propose également à ses adhérents un accès gratuit à une plateforme de veille en cybersécurité opérée par son partenaire XMCO.

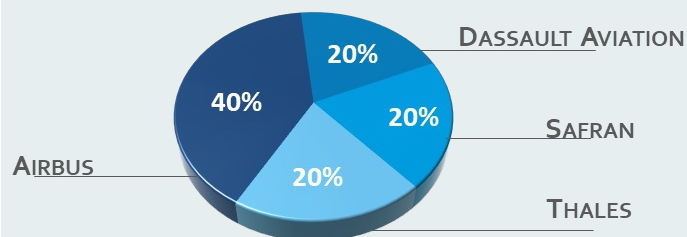
Pour en bénéficier, adhérez et/ou écrivez à : contact@cert-aviation.fr

Points sur les groupes de travail & comités : *Cybersécurité (5/5)*

→ Mission

Implémenter des **outils et services standards, sécurisés et collaboratifs** afin d'améliorer la compétitivité et la sécurité de l'Industrie Aérospatiale et Défense Européenne

→ Actionnaires:



Définition des niveaux :



NIVEAU GOLD

Equivalent niveau donneur d'ordre : détection d'attaque et remédiation, résilience éprouvée, gouvernance cyber sur toutes les strates de l'entreprise.
Ex: contrôles de sécurité automatiques et tableau de bord en temps réel du niveau de sécurité.



NIVEAU SILVER

Règles d'hygiène "avancées": toutes les solutions de protection du système d'information sont déployées et testées.
Ex: utilisation sécurisée d'internet, chiffrement des données, sécurité des PC / smartphones / serveurs, authentification forte, audit technique effectué, mesures correctives déployées.



NIVEAU BRONZE

Règles d'hygiène de l'ANSSI "basiques" déployées : le minimum vital pour un système d'information.
Ex: Solutions de sécurité minimum déployées (gestion des patches, Antivirus, Firewalls, Sensibilisation & formation utilisateurs, AntiSpam, chiffrement des disques durs.)

- Une entreprise complète **chaque niveau de façon indépendante**.
- Elle obtient un **pourcentage d'atteinte pour chaque niveau**.
- Il lui faut obtenir **+ de 90%** sur un niveau pour l'obtenir.
- Le niveau de maturité est Certifié « **VALIDATED** » par la première validation site. L'implémentation du plan d'action donne un nouveau niveau « **SELF-ASSESSED** », et qui peut être Certifié par une nouvelle validation sur site.



Objectif visé:

→ Surveillance différenciée des sous-traitants – réduction du nombre d'audits pour les compagnies et ses sous-traitants

Points sur les groupes de travail & comités : *Comité CSCE (Compétences de Sécurité des Conducteurs et utilisateurs d'Engins aéroportuaires)*

- Rappel des objectifs 2023:
 - ❖ Rattraper le retard au niveau des audits pris pendant la période 2020/2021 ✓
 - ❖ Auditer les nouvelles entreprises rejoignant le dispositif ✓
- Audits réalisés depuis la dernière CAT&R:
 - ❖ Aéroport de Rennes en novembre 2023 (recyclage);
 - ❖ Ladybird en décembre 2023 (initial) ;

L'ensemble des entreprises sont à jour de leur audit.

CAMAS et Aéroport de Cannes : Ces organisations ne sont plus couvertes par le comité CSCE. Un audit initial doit de nouveau être programmé.

- Audits programmés pour 2024:
 - ❖ AF Cargo (initial) & AF DGI (recyclage): septembre 2024
 - ❖ FEDEX (recyclage): juin 2024
 - ❖ Ladybird (recyclage): décision de réduire le cycle à un an suite à l'audit initial
- Dernier comité CSCE le 26 janvier 2024

Points sur les groupes de travail & comités : **CSCA** (*Collectif Sécurité Circulation Aéroportuaire*)

Actions et réunions prévues au sein du CSCA:

- **Réunion de réseau CSCA** (2 fois par an): tous les adhérents - Partage des hots spots, indicateurs clefs, process ou structures existants (ex: SGS...), remontées terrain, actions à venir
- **Evènement sécurité terrain** (2 fois par an)

Le 25 janvier 2024, le Groupe ADP, Air France, la CSAE, et la FNAM ont lancé le CSCA par la signature de la charte.

Cette collaboration vise à renforcer la sécurité et la prévention routière côté piste des aéroports Paris-Charles de Gaulle et Paris- Orly, dans un contexte de renouvellement massif des effectifs.

Lien ici vers le communiqué de presse: <https://www.fnam.fr/wp-content/uploads/2024/01/2024-01-25-Signature-Charte-CSCA.pdf>

Retour sur la première réunion de réseau CSCA du 29 février 2024:

- Présentation du collectif et du rétroplanning
- Partage de l'actualité accidentelle
- Partage de **l'événement terrain du 19 mars 2024** sur CDG (**Orly – le 25 avril**)
 - Une identité visuelle partagée: Plusieurs milliers de véhicules circulant en piste vont être logoté (via les services techniques)
 - Des animations sur le terrain pour promouvoir le CSCA et la Culture Zéro Accident (aux Parifs, Hots pots, animations en équipes ...)

Une quarantaine d'acteurs seront mobilisés dont la GTA

→ Prochaine réunion réseau du 19 septembre 2024



Points sur les groupes de travail & comités : *GT Maintenance GIPAG / SNEH (1/2)*

Suite à la demande du GIPAG, la date butoir pour le dépôt des MOE a été déplacée au 30 mars.

Dernière session le 13/02/2024 dédiée aux membres GIPAG/SNEH Part-I45

➤ Etude du MOE:

- Nous nous sommes basés sur le guide OSAC G-45-00 Edition 8 : <https://www.osac.aero/view/292847>
- L'ensemble des paragraphes du guide ont été balayés durant la réunion.

Quelques questions soulevées

- **Section 1.2 Politique de sécurité et objectifs:** Il faut rester générique et introduire des objectifs chiffrés dans la section 3.4 Surveillance de la performance de la sécurité.
- **Section 1.3 Personnel de commandement:** Il n'est pas nécessaire de mettre le suppléant dans l'organigramme cependant la procédure de suppléance est à intégrer.
- **Sections 1.10 & 1.11:**
 - Il faut lister les changements soumis à approbation de l'autorité. Il est conseillé de lister l'ensemble des paragraphes et sections de votre MOE & SGS soumis à approbation de l'autorité dans ce même tableau ; il ne faut pas lister les changements non soumis à approbation de l'autorité ;
 - La procédure de gestion des changements non soumis à approbation de l'autorité est à écrire ici. Elle est dans le guide OSAC P03-01 au paragraphe « 6.2.2. Traitement des modifications qui ne nécessitent pas une approbation d'OSAC »
- **Section 3.4 Surveillance de la performance de la sécurité:** une liste des indicateurs a été dressée.

Points sur les groupes de travail & comités : *GT Maintenance GIPAG / SNEH (2/2)*

Actions FNAM pour le prochain GCCCTA:

- Plusieurs RS OSAC refusent que la trame du guide MOE soit modifiée par les opérateurs. Or, le guide ne fait pas office d'un AltMoc. L'opérateur doit cependant définir une matrice de conformité.
- Plusieurs RS OSAC demandent aux opérateurs d'écrire dans le MOE ou MSGS la liste des changements non soumis à approbation de l'autorité alors qu'il faut seulement écrire la procédure.
- L'information de report au 30 mars du dépôt des MOE n'a pas été transmise correctement aux RS OSAC.
- Une date de butée avec une durée de 3 mois est donnée pour les écarts de transition alors que la date de mise en œuvre du règlement Part-145 est au 02/12/2024 (même s'il est possible de demander une extension de 3 mois supplémentaire).

Le compte-rendu du dernier GT vous sera envoyé.

Ordre du jour

1^{ère} partie

Point réglementaire

- ❖ Présentation par Olivier Outtier (DSAC) sur le rôle et les travaux du pôle Coopération Européenne et Réglementation de Sécurité
- ❖ Opinion 01-2024: Ground Handling Requirement
- ❖ NPA 2023-10: Part-147
- ❖ Workshop EASA: Fatigue Risk Management (FRM)

2^{ème} partie

Point sur les groupes de travail & comités

- ❖ Cybersécurité
 - ❖ Groupe de travail
 - ❖ Part-IS - Part IS allégée
 - ❖ Exercice de Coordination de Crise du CCTA
 - ❖ CERT Aviation France
 - ❖ AirCyber de BoostAerospace
- ❖ Comité CSCE
- ❖ CSCA
- ❖ GT Maintenance GIPAG/ SNEH

3^{ème} partie

Sujets en cours

- ❖ DSNA: Implémentation de 4-Flight
- ❖ Mesures JO:
 - ❖ Retour sur les COMEX de Coordination des Aéroports
 - ❖ Mesures de sûreté

4^{ème} partie

Points divers et problématiques

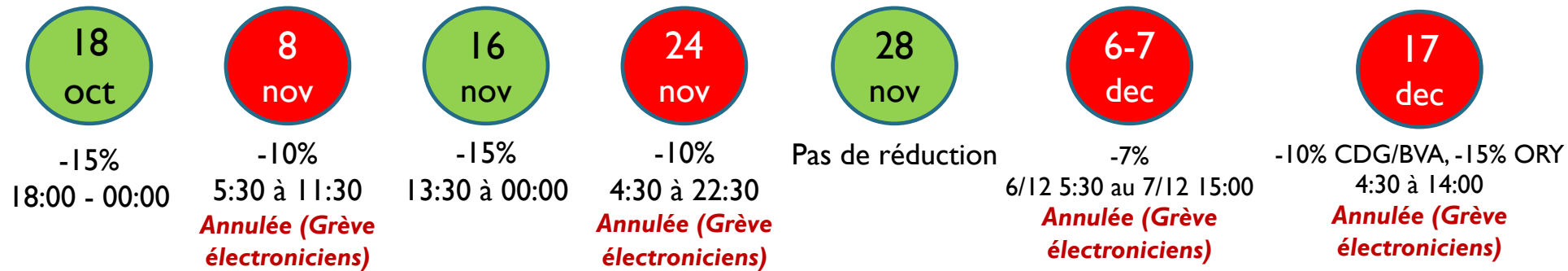
- ❖ Point divers
- ❖ Séance d'échange et tour de table

Sujets en cours : *DSNA – Implémentation de 4Flight (1/2)*

■ Focus sur Paris ACC

→ Date de mise en service reportée : 05.11.2024

1^{ère} phase de tests en situation réelle (UOP):



Heures en UTC
Aéroports :
CDG/BVA/ORY

→ **376 vols ont été annulés sur CDG/ ORY/ BVA sur les 4 jours de grève**

Sujets en cours : *DSNA – Implémentation de 4Flight (2/2)*

■ Focus sur Paris ACC

→ Date de mise en service reportée : 05.11.2024

2^{ème} UOP (longue) :

- Du 9 janvier au 14 février
- BVA et LBG ont été coordonnés durant cette période
- Sur CDG, ORY, LBG et BVA, baisse temporaire des paramètres de coordination (-30%) & historiques de compagnies préservés

A cause de problèmes techniques aux interfaces du système, par mesure de sécurité, la DSNA a décidé d'annuler l'UOP longue de 4-flight à compter du 19 janvier 2024.

Après résolution des problèmes techniques, l'UOP a repris le 26 janvier jusqu'à la fin de la période.

7 jours annulés sur les 37 initialement prévus.

3^{ème} UOP:



Après consultation des compagnies, la FNAM a envoyé un courrier (co-signé BAR & SCARA) à la DSNA demandant un report de la mise en œuvre de 4-Flight au **6 janvier 2025**.

Objectifs:

- Limiter l'impact économique du dernier trimestre de l'année ;
- Minimiser les risques qu'une mise en œuvre difficile de 4-Flight ne vienne perturber la période des congés de fin d'année;
- Eviter un deuxième épisode de pertes importantes au cours de la même année calendaire pour des acteurs fragilisés.

Points sur les groupes de travail & comités : *Mesures JO (1/9)*

Retour sur les COMEX de Coordination des Aéroports: Aéroport de Marseille Du 12 juillet au 11 août 2024

■ Parking:

Pour toutes rotation avec un turnaround de plus de 60 min, Cohor va allouer les slots en fonction de la disponibilité parking.

Paramètres de coordination :

Local hours	Arrivals per hour	Departures per hour	Total per hour
0h – 5h59	5	7	9
6h – 6h59	9	15	15
7h – 8h29	12	15	20
8h30 – 8h59	18	15	26
9h – 17h29	22	22	-
17h30 – 21h29	18	15	26
21h30 – 22h59	12	15	20
23h – 23h59	9	15	15

Points sur les groupes de travail & comités : *Mesures JO (2/9)*

Retour sur les COMEX de Coordination des Aéroports: Aéroport de Lille Du 22 juillet au 14 août 2024

■ Parking:

Pour toutes rotation avec un turnaround de plus de 60 min, Cohor va allouer les slots en fonction de la disponibilité parking.

Paramètres de coordination :

Local hours	Arrivals per hour	Departures per hour	Total per hour
0h - 23h59	10 including a maximum of 8 for commercial aviation	12 including a maximum of 8 for commercial aviation	22 including a maximum of 13 for commercial aviation and a maximum of 9 for general and business aviation

Points sur les groupes de travail & comités : *Mesures JO (3/9)*

Retour sur les COMEX de Coordination des Aéroports: Aéroport de Bordeaux
Du 23 juillet au 04 août 2024

Paramètres de coordination :

Local hours	Arrivals per hour	Departures per hour	Total per hour
0 h - 23h59	12	12	24

Points sur les groupes de travail & comités : *Mesures JO (4/9)*

Retour sur les COMEX de Coordination des Aéroports: Aéroport de PARIS - LE BOURGET Du 12 juillet au 16 septembre 2024

Périodes orange et verte:

Période verte du 12 juillet au 16 septembre sauf aux dates suivantes sous période orange:

- 3, 4, 5, 10, 11, 12 Août 2024
- Du 19 juillet au 28 juillet 2024

**** non officiel pour le moment, les périodes peuvent bouger**

Paramètres de coordination :

Paramètres nominaux pour l'aéroport du Bourget (LBG)

HEURES LOCALES	PÉRIODE VERTE *			PÉRIODE ORANGE *		
	ARRIVÉES PAR HEURE	DÉPARTS PAR HEURE	TOTAL PAR HEURE	ARRIVÉES PAR 20 MINUTES	DÉPARTS PAR 20 MINUTES	TOTAL PAR HEURE
0H - 5H59	10	10	20	4 (1)	4 (1)	20
6H - 21H59	24	24	40	8	8	40
22H - 23H59	18	18	30	6	6	30
23H - 23H59	10	10	20	4 (1)	4 (1)	20

Le signe 4 (1) signifie que, au cours de la tranche horaire correspondante, au plus 4 mouvements peuvent être acceptés sur 1 période de 20 minutes consécutive et 3 mouvements pendant 2 autres périodes de 20 minutes, sous réserve du respect des autres contraintes.

Points sur les groupes de travail & comités : *Mesures JO (5/9)*

Retour sur les COMEX de Coordination des Aéroports: **Cérémonie d'ouverture**

ORY (loc)	ARR	DEP	TOT
16h30 – 17h29	23	25*	48
17h30 – 23h29	0	0	0
...			
6h – 6h59	10	20*	25*

LBG (loc)	ARR	DEP	TOT
16h30 – 17h29	x	x	x
17h30 – 23h29	0	0	0
23h30 – 23h59	0	5	5
0h00 – 0h29	0	10	20
0h30 – 0h59	5		

CDG (loc)	ARR	DEP	TOT
16h30 – 17h29	49	43	92
17h30 – 23h29	0	0	0
23h30 – 23h49	0	5	5
23h50 – 23h59	0	7	7
0h00 – 0h29	0	20	32*
0h30 – 0h59	20		
1h00 – 1h29	20	25	32*
1h30 – 1h59			

* réflexion à mener pour augmentation

Fin de tolérance départs : 1h30 loc
Fin de tolérance arrivées : 2h00 loc

Restrictions for Friday 26th July 2024

Airport	14:30 UTC	15:30 UTC	16:30 UTC	22:00
	No increase base SRD 15 dec. 2023	No slots	Activation of the Temporary Prohibited Area NO FLIGHTS	
CDG				
LBG				
ORY				
BVA				

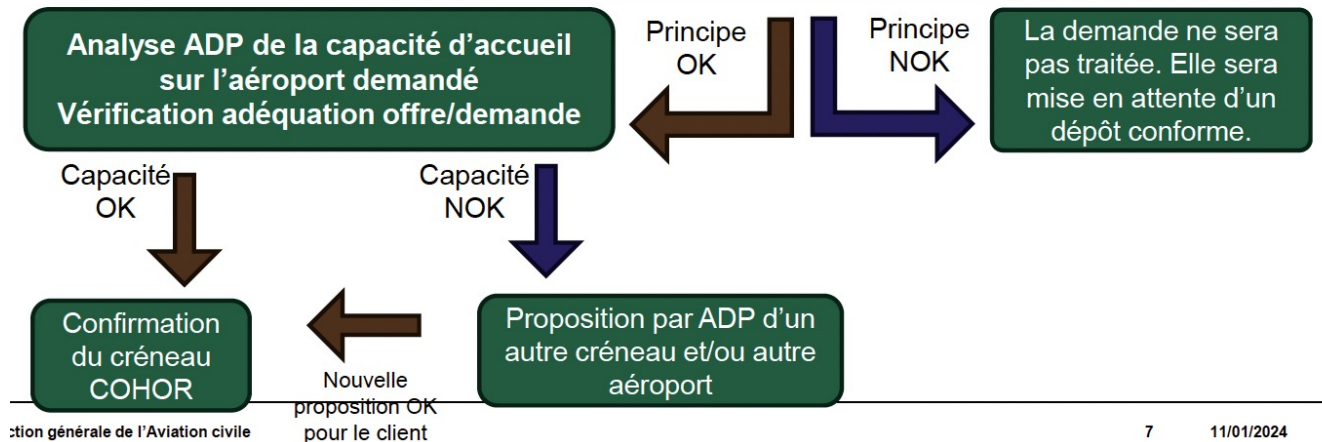
End of service for ORY and BVA

Points sur les groupes de travail & comités : *Mesures JO (6/9)*

Retour sur les COMEX de Coordination des Aéroports: Process de coordination LBG/CDG/ORY

Principes de dépôt pour les vols supplémentaires opérant entre le 12 Juillet et le 16 Septembre :

- Dépôt des programmes de vol dès qu'ils sont connus **et au plus tard à J-7**
- Dépôt de la demande de vol **au format rotation** : un vol arrivée doit être déposé avec un vol départ
- Dépôt avec un temps de rotation **maximum de 5 heures**



Problématique des dépôts de programmes de vols au plus tard à J-7 pour l'aviation d'affaires

Additional requirements on all airports

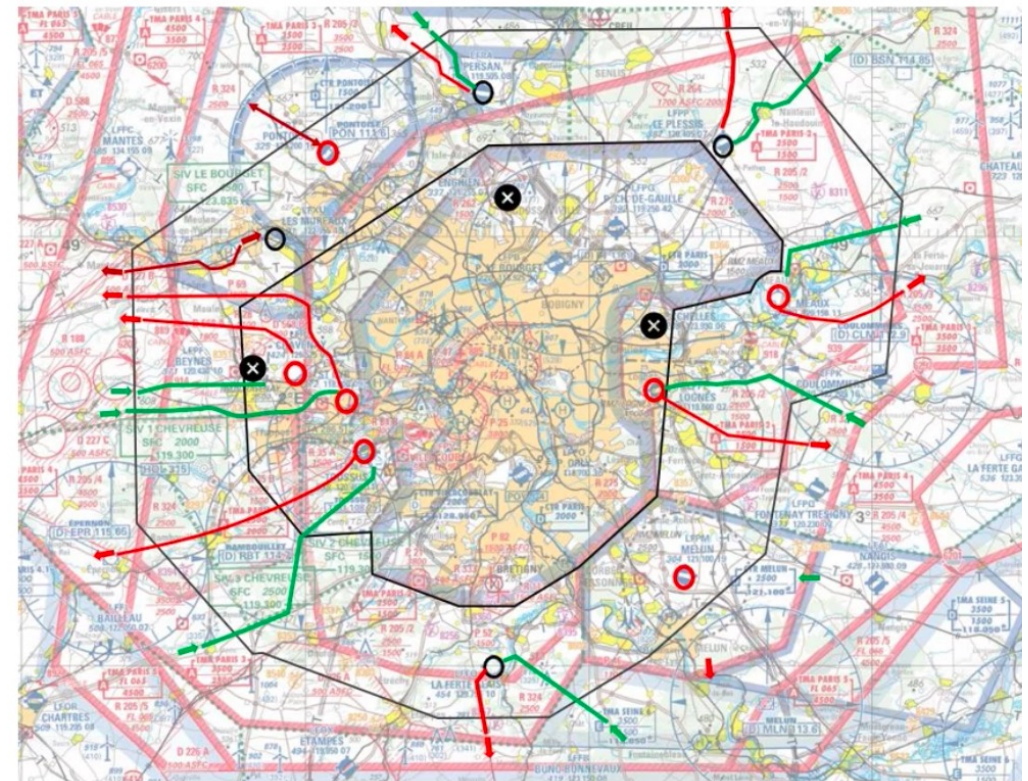
- Indicate event related slots via SCR
- Slot request for :
 - **Commercial Olympics related flights** : turn-around format with service type O
 - **Diplomatic flights** : turn-around format with service type U (E or W TBC)
 - **State flights** : turn-around format with service type E
 - **Other private flights** : turn-around format with service type D or N
- Indicate if dignitaries transported
- Due to an increase in the need of aircraft parking spaces, **plan shorter rotation times**

Points sur les groupes de travail & comités : *Mesures JO (7/9)*

Mesures de sûreté

1. Modalités de contrôle dans la ZIT et volumes max sur chaque terrain (+ cas particulier d'Issy-les-Moulineaux)

- ✓ ZIT : Vols possibles si ATS et membre réseau de confiance
- ✓ ZRT : Vols possibles en auto-info si membre réseau de confiance
- ✓ Flux maximal pour chaque terrain en cours de détermination sur chaque terrain
- ✓ Sectorisation, plan de fréquences, IFF à finaliser...
- ✓ Trajectoires dans la ZIT et ZRT :
 - Déterminer trajectoires VFR autorisées pour Le Bourget, Brétigny et Issy
 - Etudier les trajectoires HLO « intra-ZIT » autorisées afin d'éviter les sites olympiques ouverts
 - Etude du cas particulier des VTOL en aparté selon les mêmes principes que les HLO, avec PP
- ✓ Cas particulier d'Issy :
 - Limiter l'activité à Issy aux Hélicoptères « Basés » - « Enrôlés ».
 - Renforcer les mesures de sûreté générales au sol - Passage à l'inspection filtrage pour ceux qui n'ont pas de carte de circulation de l'AD (passagers en particulier)



Points sur les groupes de travail & comités : *Mesures JO (8/9)*

Mesures de sûreté

2. La mise en place de procédures d'urgence et l'identification des missions prioritaires et des POC associés

- ✓ Cas normal pour l'aviation générale :
 - ✓ J-7 : Demande de vols via le réseau de confiance
 - ✓ J-4 : Envoi de la synthèse de la programmation d'un aérodrome au C3MOA
 - ✓ J-1 à midi : Envoi des autorisations aux usagers et différents organismes – centres d'opérations
- ✓ Procédure d'urgence = après J-1 midi
- ✓ Exemples de vols particuliers : reprogrammation OBS, forces d'intervention, secours, vols d'autorités, RTE...
- ✓ Principe = le C3MOA est le point focal des demandes pour intégrer le vol prioritaire dans une programmation optimisée (sécurité des vols, sûreté)
 - Processus d'enrôlement des pilotes, machines et personnels de bord en amont des JOP
 - Carte quotidienne des zones actives (JOP, activité aérienne particulière autorisée) et des POC quotidiens d'astreinte (dont réseau de confiance)
 - Le C3MOA interagit avec son premier cercle du réseau de confiance (géographique ou thématique) pour faire les adaptations nécessaires
- ✓ Travail sur la rédaction d'un **protocole interservices** dans lequel seront décrites les procédures de travail, les POC et le fonctionnement du C3MOA

**C3MOA : centre de coordination civilo-militaire des opérations aériennes*

Points sur les groupes de travail & comités : *Mesures JO (9/9)*

Publication aéronautique

- Objectif de finalisation du dossier de documents (SUP-AIP et AIC) à passer en consultation des usagers :

14 mars 2024

Réseau de confiance

- Les réunions organisées au niveau de l'ensemble des plateformes aéroportuaires d'aviation générale franciliennes a permis d'initier la réflexion, plateforme par plateforme, sur la mise en place du « réseau de confiance » indispensable à la réalisation des vols
- Les mois à venir permettront de consolider la mise en place de ce réseau de confiance et de préparer et faire signer par chaque membre de ce réseau une charte décrivant le rôle de ces acteurs

Accréditations JO des personnels d'assistance en escale intervenant sur l'enregistrement déporté

- Inquiétude sur les difficultés à déclarer l'ensemble des personnels à Paris 2024 avant fin avril

Ordre du jour

1^{ère} partie

Point réglementaire

- ❖ Présentation par Olivier Outtier (DSAC) sur le rôle et les travaux du pôle Coopération Européenne et Réglementation de Sécurité
- ❖ Opinion 01-2024: Ground Handling Requirement
- ❖ NPA 2023-10: Part-I47
- ❖ Workshop EASA: Fatigue Risk Management (FRM)

2^{ème} partie

Point sur les groupes de travail & comités

- ❖ Cybersécurité
 - ❖ Groupe de travail
 - ❖ Part-IS - Part IS allégée
 - ❖ Exercice de Coordination de Crise du CCTA
 - ❖ CERT Aviation France
 - ❖ AirCyber de BoostAerospace
- ❖ Comité CSCE
- ❖ CSCA
- ❖ GT Maintenance GIPAG/ SNEH

3^{ème} partie

Sujets en cours

- ❖ DSNA: Implémentation de 4-Flight
- ❖ Mesures JO:
 - ❖ Retour sur les COMEX de Coordination des Aéroports
 - ❖ Mesures de sûreté

4^{ème} partie

Points divers et problématiques

- ❖ Point divers
- ❖ Séance d'échange et tour de table

Points divers

- **Retour sur le PARAC (Pôle d'analyse du risque pour l'aviation civile) du 4 mars 2024**
- **EASA Safety Week: Lien ici pour s'enregistrer** <https://easa-webmeetings.webex.com/webappng/sites/easa-webmeetings/webinar/webinarSeries/register/dedb613cbbd4427089f9e4a84cc0a734>
 - **Day 1: 22/04/2024** – Introduction and Top Safety Issues: 10:00 - 11:30 CET (UTC +1)
 - **Day 1: 22/04/2024** – Aerodromes and Ground Handling: 14:00 - 15:30 CET (UTC +1)
 - **Day 2: 23/04/2024** – Air Operations 10:00 - 11:30 CET (UTC +1)
 - **Day 2: 23/04/2024** – ATM/ANS: 14:00 - 15:30 CET (UTC +1)
 - **Day 3: 24/04/2024** – ATO/ Flight Crew Training: 10:00 - 11:30 CET (UTC +1)
 - **Day 3: 24/04/2024** – Continuing Airworthiness: 14:00 - 15:30 CET (UTC +1)
 - **Day 4: 25/04/2024** – Cyber/ Security: 10:00 - 11:30 CET (UTC +1)
 - **Day 4: 25/04/2024** – Safety Leadership: 14:00 - 15:30 CET (UTC +1)
- **Les prochaines CAT&R se dérouleront aux dates suivantes:**
 - 27 juin 2024;
 - 07 novembre 2024;

Séance d'échanges et tour de table



Echanges et tour de table sur les problématiques actuelles



Fédération
Nationale de l'Aviation
et de ses Métiers

MERCI

Toute utilisation ou reproduction intégrale ou partielle faite sans le consentement de la FNAM est illicite. Toute utilisation ou reproduction par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les dispositions des articles L.335-1 et suivants du Code de la Propriété Intellectuelle et, de manière générale, une atteinte aux droits de la FNAM.

FNAM 22, avenue Franklin Delano Roosevelt F75008 PARIS | T: +33.1.86.64.12.34

© FNAM 2008-2024



**MINISTÈRE
CHARGÉ
DES TRANSPORTS**

*Liberté
Égalité
Fraternité*



DSAC/ERS

DIRECTION DE LA COOPÉRATION EUROPÉENNE ET RÈGLEMENTATION DE SÉCURITÉ

Présentation à l'occasion de la
Commission Affaires Techniques et Règlementaires
de la FNAM du 14 mars 2024

LA DSAC

Une mission

Autorité nationale de surveillance

- => Certification et surveillance des opérateurs
- => Promotion de la sécurité

ET

- => Réglementation de sécurité :
 - **Elaboration de la réglementation nationale**
 - **Coopération européenne et internationale**



**Mission de la Direction de la Coopération Européenne
et Règlementation de Sécurité**

Direction ERS

Périmètre

Une vingtaine de personnes, dédiées à la réglementation de sécurité :

Navigabilité (initiale et continue)

Opérations aériennes

Personnels aviation civile (PN, ATCO)

Aérodrome, SSLIA, assistance en escale

Ambitions :

- conforter sa position d'acteur et de contributeur de premier plan au sein du système européen du transport aérien
- porter ses positions en Europe et dans le monde

Direction ERS

Missions principales à l'international

OACI

Coopération avec l'Organisation de l'Aviation Civile Internationale (OACI) à Montréal

- Préparation et participation aux conférences, Assemblée OACI, et à différents « Panels » ou Groupes de Travail (GT), sur les sujets de navigabilité, opérations aériennes, aéroports, licences ou encore drones,
- Suivi des amendements aux Annexes de l'OACI et rédaction des réponses aux Lettres aux Etats,
- Auto-évaluation de la DSAC pour la conformité aux normes et recommandations de l'OACI.

Direction ERS

Missions principales à l'international

DG-MOVE
EASA

Coopération avec l'Agence de l'Union Européenne pour la
Sécurité Aérienne (AESA) à Cologne et la Commission
Européenne à Bruxelles

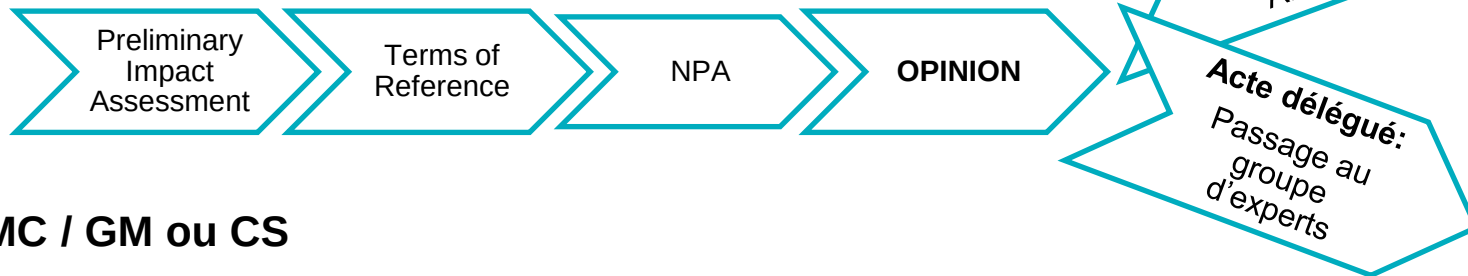
- Participation et coordination des experts pour les tâches réglementaires (RMT= Rule Making Task),
- Réponses aux consultations de l'AESA (projets de texte ou enquêtes),
- Participation aux instances représentatives des autorités (MAB = Member States Advisory Body ; TeB = Technical Bodies),
- Préparation et participation au Comité AESA (vote des projets d'actes d'exécution), au groupe d'experts (avis sur les projets d'actes délégués) et au Conseil d'Administration de l'Agence.

Direction ERS

Missions principales à l'international

Les différentes étapes du processus d'élaboration réglementaire

ACTE DÉLÉGUÉ / ACTE D'EXÉCUTION



AMC / GM ou CS



Direction ERS

Faire face aux évolutions

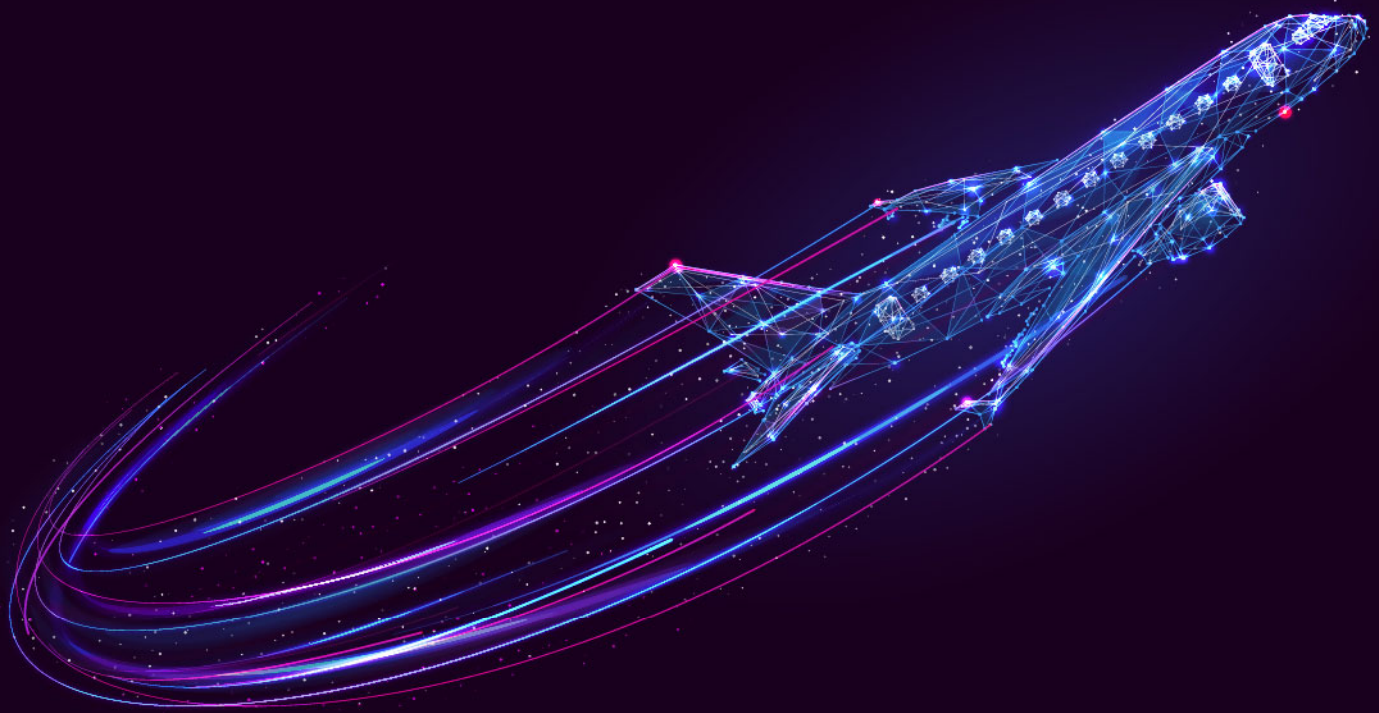
DSAC
--
FNAM

Comment mieux travailler ensemble ?

- Besoin de votre expertise et expérience de terrain (participation à des groupes internationaux, évolutions nationales)
- Remontées fédérées des usagers sur les besoins d'évolutions réglementaires
- Avoir de la visibilité sur les textes en projet et leur avancement

Examining the Need for Cybersecurity Training for Pilots

Experiment Report



June 2023



Cyber Israel
National Cyber Directorate

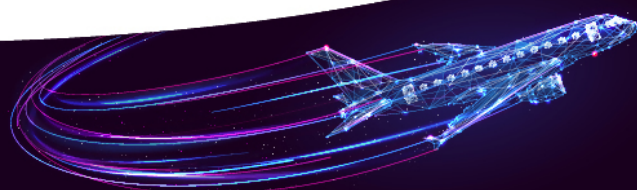


DSAC



Table of Content

I. Introduction	3
II. Research Question	4
A. Hypothesis and Counter-Hypothesis	4
B. Expected Competencies	5-6
III. Framework	7-8
IV. Experiment Description	9
A. Technical Flight Details	9
B. Flight Events	10
C. Simulated Cyber Attacks	11-15
D. Data Gathering	16
E. Data Analysis Methodology	17-18
V. Results	19
A. Analysis of the results by direct observation	19-21
B. Analysis of the results using the 3Rs method	21-23
VI. Discussion	24
A. The effectiveness of cybersecurity training for aircrews	24
B. Coping with different types of cyber-attacks	24-25
C. Extending aviation cybersecurity training	25
VII. Conclusion	25
VIII. Authors	26



I. Introduction

As modern passenger planes become more digitized and connected, the cyber-attack surface grows accordingly. What was once only a futuristic threat is now an intimidating reality. Manufacturers, operators and regulators increase their attention and investment in improving airplanes' cyber resilience, however no system is foolproof and no defense is unsurmountable. The attackers too are becoming increasingly advanced, and therefore the working assumption must be that a cyber-attack on a commercial plane is only a matter of time. When that time comes pilots may find themselves as the last line of defense.

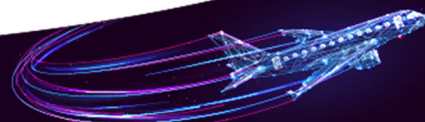
In its Cybersecurity Action Plan¹ ICAO called for Member States and Industry to develop appropriate role-based aviation cybersecurity training requirements at all levels within their organizations (CyAP 7.2). Considering the key role pilots play in aviation it is crucial to include them in this effort. More specifically, pilots may face cyber-attacks that manifest on the aircraft and may lead to increased safety risk as was demonstrated in previous work²³. However as adding any type of training for pilots is a significant undertaking for airlines it is important to approach this concept in a thoughtful manner and carefully examine just how effective cyber security training is for pilots, and what type of training would be most appropriate.

This report summarizes an experiment conducted by the Civil Aviation Authorities of Israel (CAAI) and France (DGAC), the Israel National Cyber Directorate (INCD) and ASL Airlines France, aiming to examine the need for cybersecurity training for pilots. It is meant to provide further insight on this important topic, in order to assist aviation stakeholders in their decision-making processes on this matter.

¹ <https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf>

²Safety vs. Security: Attacking Avionic Systems with Humans in the Loop; Matthew Smith, Martin Strohmeier, Jon Harman , Vincent Lenders, and Ivan Martinovic; Department of Computer Science, University of Oxford; <https://arxiv.org/abs/1905.08039>

³ Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior; Patrick Gontar, Hendrik Homans, Michelle Rostalski, Julia Behrend, Frédéric Dehais, Klaus Bengler; <https://www.sciencedirect.com/science/article/abs/pii/S0969699717300510>



II. Research Question

In this experiment the participating organizations set out to test the following issue:

Is there a performance gap in the way pilots cope with cyber security incidents onboard their aircraft, and if so how can prior training contribute to closing this gap?

A. Hypothesis and Counter-Hypothesis

Hypothesis: it is possible to promote appropriate crew responses to cyber-attacks using dedicated cyber security training.

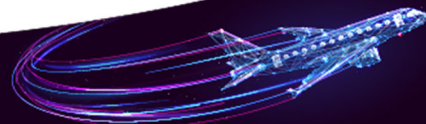
Assumption: the current generic know-how and training of the crews are insufficient to allow proper handling of cyber-attacks.

Test of the hypothesis: two groups of crews (test and control) are confronted with the same flight scenarios which include cyber-attacks.

Validation of the hypothesis: trained crews would produce expected behaviors more often than control group, and would therefore be better adapted to deal with cyber-attacks.

Counter Hypotheses:

- 1) the know-how available to "standard" crews (airmanship, generic skills in cooperation, decision making, situational awareness, etc.), allow them to cope with cyber-attacks in a satisfactory manner
 - a. The performance in dealing with situations could be the same in the face of the difficulties encountered by the test and control groups.
 - b. The two groups would not show a significant difference in the three types of behavior sought (quantitative and qualitative data).
 - c. Malicious origin identification will be weak or non-existent for the Test Group
- 2) The training provided does not improve the performance of the Test group in a noticeable manner.



B. Expected Competencies

Competencies result from interactions between: (i) knowledge, (ii) routinized action sequences and (iii) specific activity frameworks. Competencies are developed through training and experience.

The proposed hypothesis assumes that the competencies acquired by a crew could be enhanced for dealing with cyber-attacks if cyber awareness is achieved using e-learning training provided to the crew.

The counter-hypotheses respectfully assume that either:

1) general competencies would be sufficient to detect, identify and build an appropriate response to a cyber-attack. The responses of the two groups would then be equivalent with a high level of efficiency. The components of the skills already acquired would be transposed to the cyber-attack situation (knowledge, routines and specific framework).

2) the provided training is not sufficient to enhance the Test Group's competencies, and a similarly low level of competencies would be observed for the two groups. We have to keep in mind that it may be a question of lack of knowledge, inappropriate routines or a specific poorly identified activity framework.

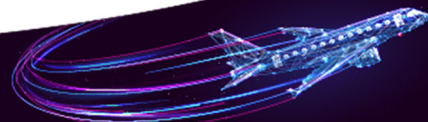
Behaviors are evaluated for the following three stages (sensemaking model):

- 1) Detection of an attack
- 2) Identification of the nature and consequences of the attack
- 3) Development of an adaptive strategy and decision

Their degree of adaptation will be objectified by collecting the following data:

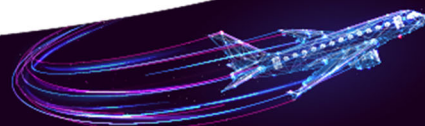
- Quantitative for each step: reaction time, implementation times, origin and number of speaking turns, etc.
- Qualitative: precision and clarity of the descriptions of each of the stages, consensus within the crew, efficiency and follow-up of actions, etc., responses produced during post-session interviews

It should be noted that the protocol and the number of pilots available for the study do not allow access to a high degree of statistical significance. Therefore, this paper presents a qualitative rather than quantitative experiment. Nevertheless, the objective remained to



carry out a "clean" study, robust, and therefore opposable to other possible data. This would be achieved if several robustness criteria are satisfied:

- Use of an "empirical" approach ("structured" verification of known behavioral models). Trends and effects observed will confirm these models and will base the conclusions and comparisons with other work carried out or studies to come.
- Repeatability of the scenario (traceability, transparency, completeness of explanations)
- Relevance and validity of the data collected and their processing



III. Framework

This study aims to test the usefulness of dedicated cyber security training for aircrews.

Two types of training were originally considered:

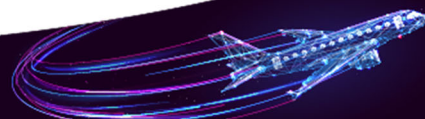
1. Theoretical training (e.g. in-class, e-learning)
2. Simulator training

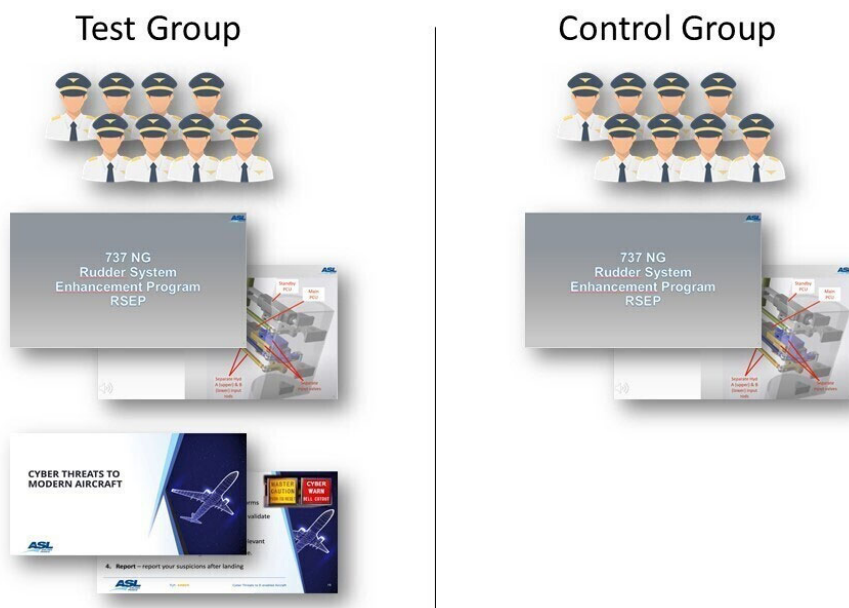
Due to practical constraints the training was eventually limited to a **self-reviewed cybersecurity e-learning deck**.

The experiment included eight crews of two-pilots each (16 pilots total). The participating crews were brought to fly a standard simulator session under false pretenses, i.e. they were *not aware* that they were participating in an experiment that had to do with cybersecurity. The simulator used was ASL's Boeing 737-800 simulator in SIMAERO Training Center near Charles de Gaulle (CDG) airport. It should be emphasized that the choice of simulator was based on availability, and it should not be deduced that any of the simulated scenarios are indeed relevant to the specific aircraft model.

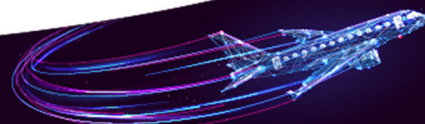


The pilots were divided (without their knowledge) into two groups – a Test Group, and a Control Group. Due to practical constraints it was not possible to provide prior simulator training to the Test Group, but rather only a self-reviewed e-learning deck. During the briefing session both groups were given e-learning decks – the Control Group received a deck about “Rudder System Enhancement Program” (RSEP) – a topic used to “obfuscate” the true nature of the experiment; The Test Group was provided with the same RSEP deck, but in addition with a deck about “*Cyber Threats to Modern Aircraft*”.





All other conditions were similar to a regular simulator session the crews are used to including flight documentation and briefing consistent with available data and practices. The ASL team leading the experimental sessions was familiar to the pilots.



IV. Experiment Description

A. Technical Flight Details

Line Oriented Flight Training (LOFT) from Lyon-Saint-Exupéry Airport (LYS) to Bergamo Airport (BGY).

Cargo flight on B737-800BCF: F-HIQB (RNP baroVNAV).

Captain: Pilot Monitoring (PM), First Officer: Pilot Flying (PF)

Weather: Runway 17R for departure, wind 220° 8 knots, visibility 4000 meters, ceiling broken 1200 ft, temperature 22°, dew point 7°, QNH 1016, runway is wet

A briefing package is available for flight preparation (ASL - 19 pages - pdf)

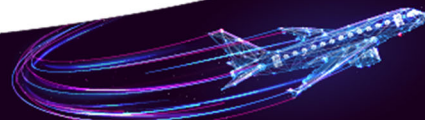
LOFT LYS BGY alt MXP

22° 220/08kt 1016

Performance Calculations: Engine Rating - 24K, Flaps 5°, Assumed temperature 35 degrees Celsius, N1 93.3%, V1 129 Kts, Vr 137 Kts, V2 143 Kts

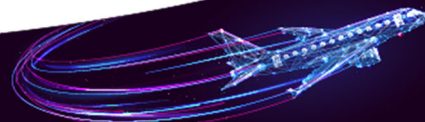
F-HIQB	Weight (kg)
Load	18200
ZFW	57652
Block Fuel	5400
Taxi	200
TOW	62852

ATIS LFLL	F-HIQB
T/O RWY 17R- A4 due to work 220/08 4000 BKN12 22°/7° 1016 WET	Parking stand (Ramp) Block Fuel 5400kg



B. Flight Events

Timing	Row	Cargo flight FPO123	Attack Num.	Nature
20 min	1	DEPARTURE BRIEFING - BEFORE TAXI & BEFORE T/O CHECK-LIST		
0h00	2	TAKE OFF RWY 17R A4 SID RISOR 2S FL70		
6 min	3	CLIMB TO FL290 STANDBY RUDDER ON		"deception" malfunction related to RSEP e-learning deck
12 min	4	CRZ ATC: CONFIRM STEADY FL290	#1	Spoofing ADSB
22 min	5	ACARS MESSAGE WITH FALSE ZFW = 52880KG	#2	Falsified Load Sheet update via ACARS
	6	ATIS BGY RNP 28 230/15 3500 B007 17°/12 1017 ILS U/S NO ELECTRICAL BACK UP		
32 min	7	DESCENT - STAR DIXER 3E – ITVUN – TIXUM FUEL INDICATORS INCREASED 200KG/MIN	#3	Spoofing fuel consumption data
46 min	8	RNP Y 28 GPS POSITION DRIFT FAST 5Nm BEFORE TIXUM APPROACHING ME541 « CONFIRM ESTABLISHED ON FINAL RNP 28? »	#4	GPS Spoofing
52 min	9	GO AROUND 4000FT GPS MALFUNCTION CANCELED 10KM B2000		
70 min	10	RDR TO FINAL FOR VISUAL PATTERN 28 FALSE EGPWS WARNING AT 1700FT	#5	False EGPWS warning
	11	LANDING		



C. Simulated Cyber Attacks

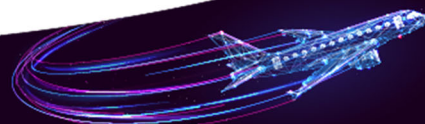
The five cyber-attacks simulated in the experiment were chosen for a set of reasons related to the experiment focus which was testing the human-factor and the effectiveness of cybersecurity training for aircrews. The focus was **not** technical and therefore there was no intention to “prove” the technical validity of these attacks as part of this study, nor their relevancy to the aircraft model used in the simulator.

The criteria used when choosing the scenarios were as follows:

1. **Detectable Attacks** – attacks that manifest in a way that may potentially be detected by the crew. An attack that is completely covert and does not manifest in the aircraft in any way is not relevant to test pilot response.
2. **Actionable Attacks** – attacks for which pilot actions are relevant. An attack where pilot actions will have no effect is not relevant for this experiment.
3. **Different from Malfunctions** – attacks that do not manifest as standard malfunctions for which the crew would simply execute an existing checklist.
4. **“Reasonable” Attacks** – we did not choose extremely dramatic or unrealistic scenarios (e.g. shutting off an engine or taking over flight controls). As mentioned before the study’s focus was not on proving just how difficult or easy these attacks are to perform, thus we chose to remain within “believable” boundaries.

1. Attack #1 – ADS-B Signal Spoofing

Description: during the cruise phase an attacker is broadcasting a fake ADS-B signal to the ground-based controller, so that the controller sees the aircraft as if it is in a wrong altitude (controller sees the aircraft as if it is flying at 28,500’ while actually the aircraft is flying at 29,000’ as requested). Once the crew changes frequency to the next ground controller the issue is resolved as the spoofing is locally targeting the first controller.



Rationale: this scenario addresses the fact that the ADS-B protocol is not secure (non-encrypted, non-authenticated) and can therefore be relatively easily spoofed⁴⁵⁶⁷⁸ The attacker's goal is to disrupt operations by creating confusion between aircraft and ATC, and possibly try to get the aircraft to fly in a wrong altitude.

Simulation Method: controller reports "Steady FL290, ATC reads 285, check altimeter setting".

Potential Pilot Actions:

1. Trust aircraft indications
2. Crosscheck three altimeters
3. Conduct dialog with controller
4. Safe side - declare "Unable RVSM" and request descent to FL280
[RVSM - Reduced Vertical Separation Minimum – allows reduction of vertical separation above Flight Level 290 from 2000-ft minimum to 1000-ft minimum]
5. Suspect ADS-B issue / spoofing (unlikely)

2. Attack #2 – Fake ACARS Message with False Load Sheet Update

Description: during the cruise phase an ACARS message is received which indicates that the Zero Fuel Weight provided on dispatch (57652 kg) was wrong, and a new ZFW value (52880 kg) should be entered to the aircraft avionics systems. It should be noted that the original value is more to the safe side as it imposes broader safety speed margins (on account of efficiency).

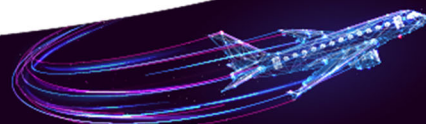
⁴ Thabet Kacem, Duminda Wijesekera, Paulo Costa, and Alexandre Barreto. "An ADS-B Intrusion Detection System". In: *2016 IEEE Trustcom/BigDataSE/ISPA*. 2016, pp. 544–551. DOI: 10.1109/TrustCom.2016.0108.

⁵ Xuhang Ying, Joanna Mazer, Giuseppe Bernieri, Mauro Conti, Linda Bushnell, and Radha Poovendran. *Detecting ADS-B Spoofing Attacks using Deep Neural Networks*. 2019. arXiv: 1904.09969 [cs.CR].

⁶ Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. "Controller–Pilot Data Link Communication Security". In: *Sensors* 18.5 (2018). ISSN: 1424-8220. DOI: 10.3390/s18051636. URL: <https://www.mdpi.com/1424-8220/18/5/1636>.

⁷ Sofie Eskilsson, Hanna Gustafsson, Suleman Khan, and Andrei Gurtov. "Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio". In: *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. 2020, 1B2-1-1B2–9. DOI: /10.1109/ICNS50378.2020.9222945.

⁸ Gustav Lindahl and Anton Blåberg. *Simulating ADS-B attacks in air traffic management :By the help of an ATM simulator*. 2020



Rationale: ACARS protocol is not encrypted nor authenticated. It has already been shown in prior research that false ACARS messages may target commercial aircraft⁹¹⁰¹¹. The attacker is trying to create a safety hazard (namely tail-strike upon landing or stall event during the approach) by having the crews accept falsified load sheet with a wrong weight.

Simulation Method: the following printed "ACARS message" is handed to the pilots:

```
RA 0540Z
DSP MSG CDGFP50
FROM DISPATCH.
DUE TO ERROR: NEW ZFW 52880
```

Potential Pilot Actions:

1. Do not suspect the received ACARS message and change ZFW
2. Try to contact Dispatch via ACARS or radio to get confirmation
3. Without confirmation, the crew decides to keep the initial ZFW, which is on the safe side.
4. Carefully monitor flight data
5. Report event after "landing"

3. Attack #3 - Spoofing Fuel Consumption

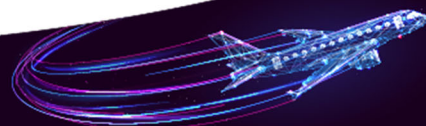
Description: during the Decent phase the aircraft fuel quantity is spoofed upwards. Fuel is increased by 200 kg per minute up to +400 kg in each wing tank.

Rationale: this is arguably the most unlikely attack, as it is both difficult to execute (requires penetrating the aircraft's avionics system), and only gains a limited effect for the attacker. However, we wanted to test an event that is outside the normal procedures and does not have a prepared checklist (unlike fuel *decrease* that may be a result of a fuel leak). From the attacker's point of view this attack is intended to create a surprise for the crew at a delicate phase of flight. An increase in workload is expected. If combined with another attack causing

⁹ Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS". In: *Financial Cryptography and Data Security (FC 2017), 21st International Conference*. April 2017. URL: file:///b3-vsrv-ctxfs01/Downloads/Tamirg/Downloads/Economy_Class_Crypto_FC17.pdf.

¹⁰ M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic. "On the Security and Privacy of ACARS". In: *Integrated Communications Navigation and Surveillance Conference (ICNS)*. Herndon, 2016.

¹¹ P. E. Storck. "Benefits of Commercial Data Link Security". In: *Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, Herndon, 2013.



a diversion to alternate airport, it may lead pilots to rely on excessive fuel they do not really have.

Simulation Method: the simulator allows changing the aircraft fuel amounts mid-flight.

Potential Pilot Actions:

1. Notice excessive fuel amount shortly after it starts
2. Notice excessive fuel amount as part of the after-go-around procedure following Attack #4
3. Never notice excessive fuel
4. After noticing excessive fuel accept this amount as available fuel
5. After noticing excessive fuel suspect fuel amount indication
6. Report event after landing

4. Attack #4 – GPS Spoofing

Description: during RNAV approach GPS is spoofed at a rate of about 0.05NM/minute (roughly 100 meters per minute). It takes about 5 minutes to exceed Actual Navigation Performance (ANP) 0.3, which is required for RNP approach. This rate is sufficiently slow to avoid crew detection until an alert occurs.

Rationale: GPS spoofing is a known hazard¹²¹³¹⁴¹⁵. An attacker may use GPS spoofing to try and create a safety hazard by spoofing the aircraft into an obstacle or to touch down before the runway, especially in Instrument Meteorological Conditions (IMC).

Simulation Method: the simulator allows GPS spoofing. After passing the FAF Tower asks: "Confirm established on final APP RNP 28"? ANP value is increasing during approach and finally alert messages "Terrain Position" and "Unable Required Navigation Performance" appear.

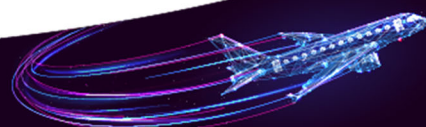
Note: "Terrain Position" is an alert related to the EGPWS system which uses a different GPS receiver from the navigation system. This alert is not part of the go around standard.

¹² Berz, G. 2018. GNSS spoofing and aviation: an evolving relationship. Inside: *GNSS*, 25 September [online]. Available at: <https://insidegnss.com/gnssspoofing-and-aviation-an-evolving-relationship>.

¹³ Morales-Ferre, R., Richter, P., Falletti, E., de la Fuente, A. & Lohan, E.S. "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft". In: *IEEE Communications Surveys&Tutorials*, 22(1), pp.249-291. Available at: <https://doi.org/10.1109/COMST.2019.2949178>.

¹⁴ Nicola, M., Falco, G., Morales-Ferre, R., Lohan, E-S., Fuente, A. de la & Falletti. "Collaborative solutions for interference management in GNSS based aircraft navigation". In: *Sensors*, 20(15), pp.4085-4108 Available at: <https://doi.org/10.3390/s20154085>.

¹⁵ Steindl, E., Dunkel, W., Hornbostel, A., Haettich, C. & Remi, P. "The impact of interference caused by GPS repeaters on GNSS receivers and services". In: European Navigation Conference (ENC) GNSS 2013, April 22-25 [online]. Available at: <https://elib.dlr.de/84739>



«UNABLE REQD NAV PERF-RNP» is a navigation-system warning which warrants a go around procedure.

Potential Pilot Actions:

1. Go around
2. Ask for radar vectors
3. Request ILS (reply: no ILS is available)
4. Request new RNP approach attempt to same runway under radar vectors or LNAV
5. Request RNP 10 or VOR 10 under radar vectors or LNAV
6. Request diversion to alternate field
7. Check aircraft systems
8. Suspect GPS jamming or spoofing
9. Ask ATC if there were any other reports on GPS issues (reply: yes, one report 10 min ago)

5. Attack #5 - False EGPWS Warning

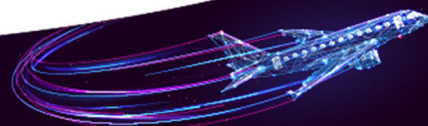
Description: after attack #4 Go Around weather conditions improve allowing a visual approach. During the Final leg of the approach, at 1700' QNH a false EGPWS "Terrain Pull up" alert is triggered, resulting from the spoofed GPS. At this point the crew has visual contact with the runway.

Rationale: one of the consequences of GPS spoofing / jamming may be false EGPWS alerts. Such alerts have been experienced in real life incidents in GPS interference areas.

Simulation Method: the simulator supports triggering such alerts at specific times.

Potential Pilot Actions:

1. Go around
2. Flying visual, crew disregards the alarm
3. Communication between PF and PM
4. After GPS spoofing, crew may relate the EGPWS alert to GPS interference



D. Data Gathering

Experiment data was collected in the following manners:

1. Video recording

Used to record raw data about:

- in-board and out-board communication
- crew actions
- durations between inputs and crew responses
- general synchronization of behaviors (verbal, gesture, action, time)

This raw data allows immediate and deferred crew behavioral analysis.

2. Observation grids

Two observation grids are used :

- A "Technical" grid to gather observations about technical behaviors
- An "Attitude" grid to collect data relating to non-technical skills

3. "Hot" Individual Debriefing

A 10 min long personal questionnaire provided immediately after the simulator flight, to be filled individually by each pilot. The questionnaire Includes:

- A short set of questions about their experience as a pilot.
- Questions regarding the flight (without mention of the possibility of cyber-attack)

4. "Cold" Debriefing Interview

An interview based on the "3R Method" - a method intended to analyze crew behavior when facing unforeseen events:

R1 - Readiness

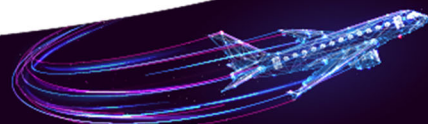
R2 - Recognition

R3 - Reaction

Crew behaviors are coded for each attack according to R1, R2 and R3.

5. Post-Experiment Survey

After the end of the experiment, a survey was sent to all crews to find out their new perception of cyber risks. Of the 16 pilots who took part in the experiment, we obtained 12 responses.



E. Data Analysis Methodology

Data was analyzed based on the Competencies Based Training and Assessment (CBTA) method.

Guidance Material CBTA IATA - 21/01:

<https://www.iata.org/contentassets/c0f61fc821dc4f62bb6441d7abedb076/competency-assessment-and-evaluation-for-pilots-instructors-and-evaluators-gm.pdf>

1. Definition of Competency

Competency: a dimension of human performance that is used to reliably predict successful performance on the job. A competency is manifested and observed through behaviors that mobilize the relevant knowledge, skills and attitudes to carry out activities or tasks under specified conditions .

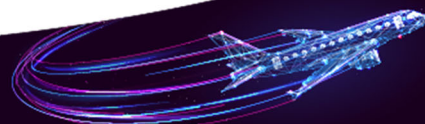
ICAO describes knowledge, skills and attitude as :

- Knowledge is specific information required to enable a learner to develop and apply the skills and attitudes to recall facts, identify concepts, apply rules or principles, solve problems, and think creatively in the context of work .
- A skill is an ability to perform an activity or action. It is often divided into three types: motor, cognitive and metacognitive skills .
- Attitude is a persistent internal mental state or disposition that influences an individual's choice of personal action toward some object, person or event and that can be learned. Attitudes have affective components, cognitive aspects and behavioral consequences. To demonstrate the "right" attitude, and a learner needs to "know how to be" in a given context .

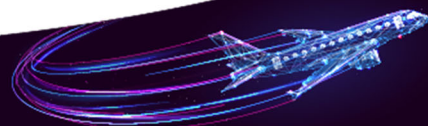
2. List of competencies

List of CBTA pilot's competencies in IATA guidance Material:

- 0 – Application of knowledge
- 1 – Application of procedures and compliance with regulations
- 2 – Communication
- 3 – Aeroplane Flight Path Management – Automation
- 4 – Aeroplane Flight Path Management – Manual
- 5 – Leadership and Team work
- 6 – Problem solving and decision-making
- 7 – Situation Awareness and management of information
- 8 – Workload management



Each of these competencies is identified using observable behaviors (OB). They are listed in IATA Guidance material.



V. Results

As discussed in section II this experiment was set up to answer the following research question:

Is there a performance gap in the way pilots cope with cyber security incidents onboard their aircraft, and if so how can prior training contribute to closing this gap?

The results were analyzed from two complementary angles using two methods:

A. Analysis of the results by direct observation

B. Analysis of the results using the "3Rs method" - a systematic method of analysis of aviation safety reports

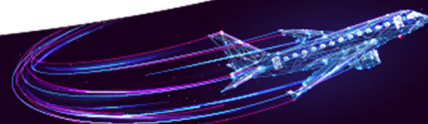
A. Analysis of the Results by Direct Observation

The study highlighted three remarkable points:

1. First result: low cyber awareness by all crews

Apart from a single mention of cyber security by one of the "trained crews", none of the eight crews understood that they were facing a series of cyber-attacks. This is true for both during the flight, and after the flight since none of the crews ever mentioned a cyber-attack as a possible cause in the debriefings. In other words, none of the crews had imagined that a commercial flight could be subject to this type of attack, and the strategies applied to continue the flight safely were chosen without identifying the threat.

This is especially noteworthy for the Test Group (the "trained crews") as these pilots were presented with an e-learning deck about potential cyber threats to aircraft just prior to boarding the simulator session. It should be noted however that the crews went over the e-learning deck on their own, without receiving guided training or any kind of emphasis. Therefore, the lack of cyber awareness may largely be attributed to the *type* of training which seems to have not made a significant impact on the crews (contrary for example to the simulator training itself as evident from point #3 below).



2. Second Result: flight safety was never compromised

The second outstanding observation was that none of the eight crews were put in any *serious* difficulty, and the safety of the flight was never compromised. While, as discussed in section IV.C, the cyber-attacks were chosen partly because they were "reasonable" and not extreme, low performance levels or alertness could still have led to increased safety risk.

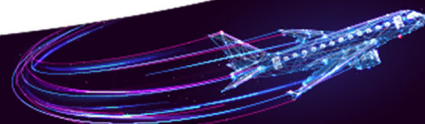
For example, in the case of attack #1 consisting of transmitting an erroneous flight level to ATC (the 3 altimeter readouts were all consistent with each other), the crews doubted their real altitude when ATC indicated that they saw them at a different altitude. Some contacted the next ATM sector, others tried to verify or ask questions. In other words, at no time did they isolate themselves from the rest of the operations, which contributed to a relevant analysis of the situation.

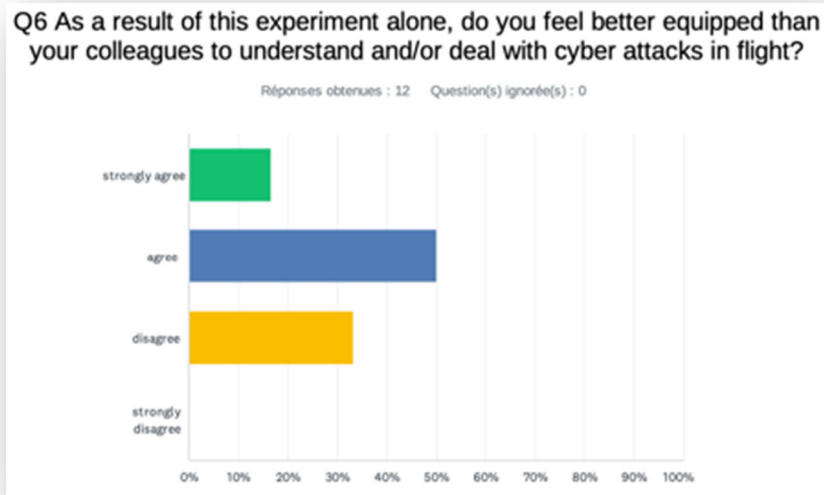
For all the attacks, the strategy of the eight crews was always to involve all the actors related to the flight, in particular ATC, to understand the situation, to cross-check information and to remove their doubts. Finally, they all correctly assessed the situation with the information available and mentioned the possible alternatives following this analysis.

3. Third Result: simulator training increased awareness to cyber threats

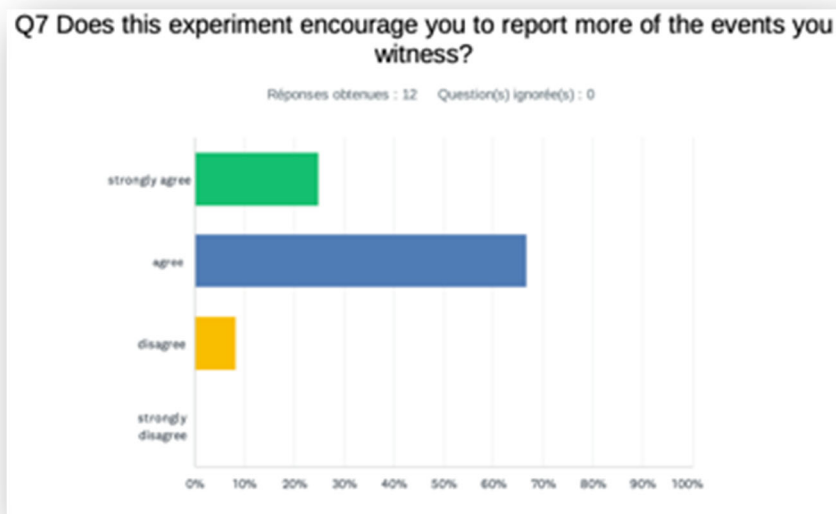
After the end of the experiment, a survey was sent to all crews to find out their new perception of cyber risks. Of the 16 pilots who took part in the experiment, we obtained 12 responses. The responses demonstrated that the experiment has led to an increased awareness of cyber threats among the crews.

a) Two thirds of the crews acknowledge that they are now more aware of the effects of cyber-attacks on flight safety. This was also expressed in the flight debriefings (hot and cold).





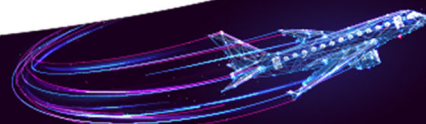
b) More than 90% of the pilots surveyed say they are now more aware of the reporting of possible cyber events.



B. Analysis of the Results Using the 3Rs Method

The 3R analysis grid has the merit of having been tested on a large scale in another context. It consists of carrying out a systematic analysis of a large number of safety reports by successively asking three simple questions about an event that occurred in flight:

- A. "Was the crew ready?" = Readiness
- B. "Did they identify the problem?" = Recognition
- C. "Did they implement the right reaction?" = Reaction.



The respective answers to these three questions are established through 4 criteria.

We first tried to average the results of the 5 types of cyber-attacks. However, despite the significantly different scores, the small sample size did not allow us to identify discriminants related to the fact that crews received a pre-flight briefing on cyber threats. Furthermore, this analysis of the results by the average masked the diversity of the types of attacks, which is why this approach did not seem relevant to us.

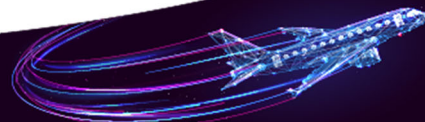
We therefore analyzed each attack to identify noticeable points by considering the dispersion of the results of the reactions to the types of attacks. This will be the focus of the analysis of the results, as shown in the following analysis using the 3R method.

	Attack #1	Attack #2	Attack #3	Attack #4	Attack #5
	ADS-B Signal Spoofing	Fake ACARS Message	Fuel Spoofing	GPS Spoofing	False EGPWS Warning
R1 - READINESS	Y	Y	Y	Y	Y
R1.1 - Fit for flight (Not fatigued, healthy?)	Y	Y	Y	Y	Y
R1.2 - Trained (Competency and currency?)	Y	Y	Y	Y	Y
R1.3 - Workload Management (Able to manage all usual situations?)	Y	Y	Y	Y	Y
R1.4 - Engaged (Involved and active?)	Y	Y	Y	Y	Y
R2 - RECOGNITION	Y	Y	N	Y	Y
R2.1 - Detection (Problem seen?)	Y	Y	N	Y	Y
R2.2 - Identification (Correct diagnostic?)	Y	Y	N	Y	Y
R2.3 - Understanding (Understanding origin of the problem?)	Y	Y	N	Y	Y
R2.4 - Recall (Knowledge of a procedure applicable?)	?	Y	N	?	Y
R3 - REACTION	Y	Y	N	Y	Y
R3.1 - Immediate (Was the problem managed on time?)	Y	Y	N	Y	Y
R3.2 - Timely adapted (Good sequencing of the actions?)	Y	Y	N	Y	Y
R3.3 - Appropriate (Correct procedure applied?)	Y	Y	N	Y	Y
R3.4 - Effective (Is the problem solved?)	?	Y	N	Y	Y

Y = yes

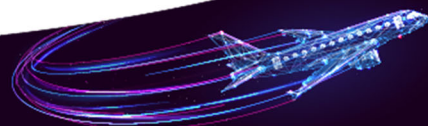
N = no

? = Unable to assess



With the 3R analysis grid, three remarkable points appear:

- a) The crews are all "fit for flight", i.e. prepared for the flight.
- b) In the case of attack #1 (ADSB), the data collected did not allow us to draw a conclusion
- c) Attack #3 (Fuel) is the attack for which there is unambiguously no recognition of the problem, and therefore no adequate reaction.



VI. Discussion

A. The effectiveness of cybersecurity training for aircrews

Even when combining the direct observation approach and a 3Rs approach, the results obtained did not display a clear differentiation in the ability to handle cyber-attacks by the Test Group (those who were presented with the cybersecurity e-learning deck) vs. the Control Group (those who were not presented with the cybersecurity e-learning deck). Both groups displayed **low awareness** to the potential threat of cyber-attacks on a commercial aircraft in-flight.

On the other hand, the direct confrontation with cyber-attacks **in the simulator** did raise the awareness of the crews of the variety and quantity of possible cyber-attacks as evident from the post-experiment survey. We therefore conclude that a self-reviewed e-learning deck is not sufficient to raise aircrews' awareness of the threat, and if such awareness is desired then more robust training is needed. Such robust training may include for example thorough class training by a professional trainer, PC-based simulator training, or full-fledged flight simulator training.

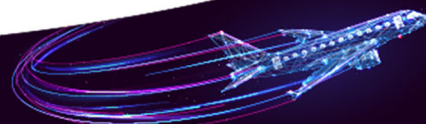
The determination whether the level of threat currently justifies investment in such training is outside the scope of this experiment and remains an open question to be examined by civil aviation stakeholders and regulators.

B. Coping with different types of cyber-attacks

As mentioned above, five types of attacks were dealt with by the crews and an analysis of the results according to the types of attacks allows us to shed further light on our results by considering the reactions of the crews in the context for which they were selected and trained, in particular to apply Standard Operating Procedures (SOP).

Indeed, attacks can be interpreted not so much according to their nature (cyber/non-cyber) but rather according to whether their consequences can be identified through an alarm or a check provided for by the SOPs. Despite the numerous alarms present on board an aircraft, there are certain situations or combinations of events for which there are no alarms and/or for which there are no SOP's. The five scenarios can therefore be divided according to the different means available to crews to identify and deal with the problem.

1. When crews have indications to react to (alarms and SOP's), all crews identify and deal with the problem correctly, according to their training. This is the case for attacks 4 (GPS Spoofing) and 5 (EGPWS). The fact that the problem is cyber related is inconsequential, because the crews know what to do without ambiguity.
2. On the other hand, when alarms and/or procedures are incomplete as in attacks 1 (ADS-B) and 2 (ACARS) with an external intervention mentioning an unexpected element, crew responses may be diverse and therefore inappropriate.
3. Finally, in the case where there is neither an alarm nor a SOP (Attack 3 - erroneous fuel value), the ability to identify the problem and deal with it is very clearly degraded.



There are three quite clearly differentiated statuses, depending on the completeness of the elements available to crews to identify and deal with a threat. When cybersecurity training for pilots is developed it should be carefully considered how pilots should be trained for these three types of scenarios. For example, given the low probability of occurrence of cyber-attacks, one must consider the risk of encouraging crews to wrongly attribute ambiguous problems or problems for which no SOP exists to a cyber cause.

C. Extending aviation cybersecurity training

This study focused on the need for cybersecurity training for aircrews. The observations and findings also suggest that awareness of the risks and effects of cyberattacks should possibly be extended to Air Traffic Control, Airline Operations and possibly other aviation stakeholders as well, as they may encounter unusual behaviors and singular questions from crews trying to interpret inconsistencies in the available data. In these situations, it is important for these entities to support pilots without doubting their skills, even when facing unique or uncommon interactions and questions.

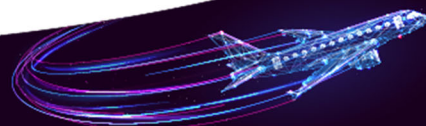
Moreover, systems operated by these entities may also be subject to cyber-attacks, an area the current study did not address.

VII. Conclusion

In this experiment we examined the need for, and the effectiveness of cyber security training for aircrews. We conclude that there is currently low awareness of this threat among all participating aircrews. We also found that a self-reviewed e-learning deck did not significantly raise this awareness. However, the simulator training itself did significantly increase the awareness of the crews to the threat of cyber-attacks.

We analyzed three "categories" of cyber-attacks based on the availability of indications and appropriate SOPs to handle the attack. Each of these categories would require different type of training. The third type – attacks that have no clear indication and no relevant SOP available, presents the biggest challenge for pilots.

It is recommended that the relevant regulatory authorities, as well as other civil aviation stakeholders, continue to monitor the growing threat of cyber-attacks on aircrafts, and the resulting need to train pilots on this emerging threat. As the likelihood of such attacks grows it is recommended to consider various training options including thorough class training, and eventually simulator training as well.



VIII. Authors

ASL Airlines France

- Captain Eymoz Franck - B737 TRI/TRE/SE, ASL Airlines France
- Geslain Marine - Deputy Flight Safety Manager, ASL Airlines France
- Captain Jacquemin Pierre - Flight Safety Manager, ASL Airlines France
- Pastorelli Ivan - Safety Management Consultant, Safety Sciences Ltd.

Civil Aviation Authority of Israel (CAAI)

- Alook Eli – Head of Regulation Department, Civil Aviation Authority of Israel (CAAI)
- Captain Molcho Moshe– Head of Air Carrier Department, Civil Aviation Authority of Israel (CAAI)

Direction Générale de l'Aviation Civile (DGAC)

- Corcos Stephane - Head safety analysis & SSP implementation, Direction Générale de l'Aviation Civile (DGAC), France
- Valot Claude– Human Factor Consultant in Risk Management
- Captain Vernay André - Human Risk Program Manager, Direction Générale de l'Aviation Civile (DGAC), France

Israel National Cyber Directorate (INCD)

- Goren Tamir– Director of Strategic Programs, Israel National Cyber Directorate

