

RAPPORT SIMPLIFIÉ D'ANALYSE DE SÉCURITÉ DES SYSTÈMES DE COMMUNICATION

Référence: RSAS-COM-2025-004 | Classification: STANDARD / USAGE INTERNE

RAPPORT SIMPLIFIÉ D'ANALYSE DE SÉCURITÉ DES SYSTÈMES DE COMMUNICATION

Référence: RSAS-COM-2025-004

Classification: STANDARD / USAGE INTERNE

Type d'aéronef: Avions commerciaux (A320/B737/E190)

Public cible: Personnel technique et opérationnel

Version: 2.3

Date de révision: 10 mai 2025

RÉSUMÉ EXÉCUTIF

Ce rapport présente une analyse simplifiée de la sécurité des systèmes de communication aéronautique, conformément aux exigences des autorités de l'aviation civile (EASA et FAA). Il identifie les risques potentiels, évalue leur impact sur la sécurité des vols et propose des mesures d'atténuation adaptées.

L'analyse a révélé que les systèmes de communication actuels présentent un niveau de sécurité globalement satisfaisant, avec quelques points d'amélioration identifiés. Les recommandations formulées permettront de renforcer davantage la résilience de ces systèmes face aux défaillances techniques et aux menaces émergentes.

1. INTRODUCTION

1.1 Contexte

Les systèmes de communication sont essentiels à la sécurité des opérations aériennes. Ils permettent l'échange d'informations critiques entre l'équipage, les contrôleurs aériens et les

opérations au sol. Toute défaillance de ces systèmes peut avoir des conséquences significatives sur la sécurité des vols.

Cette analyse s'inscrit dans le cadre du programme continu d'amélioration de la sécurité, conformément aux exigences du Système de Gestion de la Sécurité (SGS) et aux recommandations des autorités de l'aviation civile.

1.2 Objectifs

Les objectifs principaux de cette analyse sont de: - Identifier les risques potentiels associés aux systèmes de communication - Évaluer l'impact de ces risques sur la sécurité des opérations - Proposer des mesures d'atténuation adaptées - Établir des recommandations pour améliorer la résilience des systèmes

1.3 Portée de l'analyse

Cette analyse couvre les systèmes de communication suivants: - Communications vocales (VHF, HF, Interphone) - Communications de données (ACARS, CPDLC) - Systèmes de surveillance (ADS-B, Mode S) - Communications d'urgence (ELT, systèmes de secours)

L'analyse se concentre sur les avions commerciaux de type Airbus A320, Boeing 737 et Embraer E190, qui représentent la majorité de la flotte moyen-courrier mondiale.

2. MÉTHODOLOGIE

2.1 Approche d'analyse

L'analyse de sécurité a été réalisée selon une approche structurée en quatre étapes:

1. **Identification des dangers:** Recensement des défaillances potentielles et des menaces externes
2. **Évaluation des risques:** Analyse de la probabilité et de la gravité des conséquences
3. **Détermination des mesures d'atténuation:** Identification des barrières existantes et proposées
4. **Recommandations:** Formulation de propositions d'amélioration

2.2 Sources d'information

Les informations utilisées pour cette analyse proviennent de: - Rapports d'incidents et d'accidents (base de données ECCAIRS) - Retours d'expérience des équipages et du personnel de

maintenance - Documentation technique des constructeurs - Bulletins de service et directives de navigabilité - Études sectorielles sur la sécurité des communications aéronautiques

2.3 Matrice d'évaluation des risques

L'évaluation des risques a été réalisée à l'aide d'une matrice standard combinant: - **Probabilité:** De 1 (extrêmement improbable) à 5 (fréquent) - **Gravité:** De A (catastrophique) à E (négligeable) - **Indice de risque:** Combinaison de la probabilité et de la gravité

Les risques sont classés en trois catégories: - **Risque élevé (rouge):** Action immédiate requise - **Risque moyen (jaune):** Action planifiée nécessaire - **Risque faible (vert):** Acceptable avec surveillance régulière

3. DESCRIPTION DES SYSTÈMES

3.1 Systèmes de communication vocale

3.1.1 Système VHF (Very High Frequency)

Le système VHF est le principal moyen de communication entre l'équipage et les services de contrôle aérien. Les avions modernes sont équipés de deux ou trois radios VHF indépendantes opérant dans la bande 118-137 MHz.

Caractéristiques principales: - Portée: Environ 200 NM en ligne de vue - Clarté: Excellente qualité audio en l'absence d'interférences - Redondance: Multiples radios indépendantes - Alimentation: Principale et secours

Limitations connues: - Portée limitée à la ligne de vue (pas de couverture océanique) - Sensibilité aux interférences électromagnétiques - Congestion des fréquences dans les espaces aériens denses

3.1.2 Système HF (High Frequency)

Le système HF permet des communications à très longue distance, particulièrement utiles pour les vols océaniques ou polaires. Il opère dans la bande 2-30 MHz.

Caractéristiques principales: - Portée: Mondiale grâce à la propagation ionosphérique - Redondance: Généralement deux systèmes indépendants - Modes: Voix et données (HFDL)

Limitations connues: - Qualité audio variable selon les conditions ionosphériques - Sensibilité aux perturbations atmosphériques - Complexité d'utilisation par rapport au VHF

3.1.3 Interphone

Le système d'interphone permet la communication interne entre les membres d'équipage et avec les passagers.

Caractéristiques principales: - Réseau dédié indépendant des communications externes - Priorités configurables pour les appels d'urgence - Intégration avec le système d'annonces passagers

Limitations connues: - Dépendance à l'alimentation électrique de l'avion - Possibilité de défaillances localisées (postes individuels)

3.2 Systèmes de communication de données

3.2.1 ACARS (Aircraft Communications Addressing and Reporting System)

Le système ACARS permet l'échange automatisé de messages courts entre l'avion et les stations au sol.

Caractéristiques principales: - Transmission automatique de données opérationnelles - Communications avec les opérations compagnie - Surveillance des paramètres techniques - Multiples voies de transmission (VHF, HF, Satellite)

Limitations connues: - Bande passante limitée - Délais de transmission variables - Couverture dépendante du réseau de stations au sol

3.2.2 CPDLC (Controller-Pilot Data Link Communications)

Le système CPDLC permet l'échange de messages textuels entre les contrôleurs et les pilotes, réduisant la charge des communications vocales.

Caractéristiques principales: - Messages standardisés pour les autorisations ATC - Réduction des erreurs de communication - Enregistrement automatique des échanges - Intégration avec les systèmes de gestion de vol

Limitations connues: - Déploiement encore partiel dans certaines régions - Temps de réponse plus long que les communications vocales - Nécessite une formation spécifique des équipages

3.3 Systèmes de surveillance

3.3.1 Transpondeur Mode S

Le transpondeur Mode S permet l'identification précise de l'aéronef par les systèmes de surveillance au sol et les autres aéronefs.

Caractéristiques principales: - Identification unique de l'aéronef - Transmission automatique de l'altitude - Support des fonctionnalités TCAS - Capacité d'interrogation sélective

Limitations connues: - Dépendance aux interrogations des radars au sol - Vulnérabilité potentielle aux interférences

3.3.2 ADS-B (Automatic Dependent Surveillance-Broadcast)

Le système ADS-B diffuse automatiquement la position, l'altitude, la vitesse et l'identification de l'aéronef.

Caractéristiques principales: - Mise à jour de position à haute fréquence - Indépendance des infrastructures radar traditionnelles - Amélioration de la conscience situationnelle - Support de nouvelles fonctionnalités de séparation

Limitations connues: - Dépendance à la précision du GNSS - Possibilité de transmission de données erronées - Questions de cybersécurité émergentes

3.4 Systèmes de communication d'urgence

3.4.1 ELT (Emergency Locator Transmitter)

L'ELT est un émetteur qui s'active automatiquement en cas d'impact pour faciliter la localisation de l'aéronef.

Caractéristiques principales: - Activation automatique par forces G - Transmission sur fréquences d'urgence (121.5 MHz et 406 MHz) - Intégration au système Cospas-Sarsat - Batterie indépendante

Limitations connues: - Fiabilité de l'activation automatique - Durée de vie limitée de la batterie - Possibilité de destruction lors d'impacts violents

3.4.2 Systèmes de secours

Divers systèmes de secours sont disponibles en cas de défaillance des systèmes principaux.

Caractéristiques principales: - Radio VHF de secours avec alimentation indépendante - Batterie dédiée pour communications d'urgence - Procédures alternatives codifiées

Limitations connues: - Fonctionnalités réduites par rapport aux systèmes principaux - Durée d'utilisation limitée par la capacité des batteries

4. ANALYSE DES RISQUES

4.1 Identification des dangers

L'analyse a identifié plusieurs catégories de dangers potentiels:

4.1.1 Défaillances techniques

- Panne totale des systèmes radio VHF
- Défaillance des antennes de communication
- Perte de l'alimentation électrique des systèmes de communication
- Défaillance des systèmes audio (casques, haut-parleurs)
- Dysfonctionnement des panneaux de contrôle audio

4.1.2 Facteurs environnementaux

- Interférences électromagnétiques
- Conditions météorologiques sévères affectant la propagation
- Perturbations ionosphériques pour les communications HF
- Foudroiement affectant les systèmes électroniques

4.1.3 Facteurs humains

- Erreurs de sélection de fréquence
- Mauvaise interprétation des messages
- Formation insuffisante aux procédures de communication
- Charge de travail excessive limitant la capacité de communication

4.1.4 Menaces externes

- Brouillage intentionnel des fréquences
- Cyberattaques sur les systèmes de communication numérique
- Usurpation de signaux ADS-B
- Transmission de fausses informations

4.2 Évaluation des risques

Les risques identifiés ont été évalués selon la matrice de risque standard:

Danger	Probabilité	Gravité	Indice de risque
Panne totale VHF	2 (rare)	B (dangereux)	2B (moyen)

Défaillance antenne	3 (occasionnel)	C (majeur)	3C (moyen)
Perte alimentation	2 (rare)	C (majeur)	2C (faible)
Interférences EM	4 (fréquent)	D (mineur)	4D (faible)
Erreurs humaines	4 (fréquent)	C (majeur)	4C (moyen)
Brouillage	2 (rare)	B (dangereux)	2B (moyen)
Cyberattaques	2 (rare)	B (dangereux)	2B (moyen)

4.3 Mesures d'atténuation existantes

Plusieurs mesures sont déjà en place pour atténuer les risques identifiés:

4.3.1 Redondance des systèmes

- Multiples radios VHF indépendantes
- Systèmes de communication alternatifs (HF, SATCOM)
- Sources d'alimentation multiples et secours

4.3.2 Procédures opérationnelles

- Procédures de panne de communication standardisées
- Vérifications croisées des communications importantes
- Briefings spécifiques pour les zones à risque

4.3.3 Formation et sensibilisation

- Formation initiale et récurrente aux communications
- Entraînement aux situations dégradées
- Partage des retours d'expérience

4.3.4 Maintenance préventive

- Inspections régulières des systèmes de communication
- Tests fonctionnels avant vol
- Surveillance des tendances de défaillance

5. RÉSULTATS ET RECOMMANDATIONS

5.1 Synthèse des résultats

L'analyse a démontré que les systèmes de communication actuels présentent un niveau de sécurité globalement satisfaisant grâce aux multiples redondances et aux procédures en place. Cependant, certains risques méritent une attention particulière:

1. Les erreurs humaines dans la gestion des communications restent un facteur significatif
2. Les menaces émergentes liées à la cybersécurité sont insuffisamment adressées
3. La dépendance croissante aux communications numériques introduit de nouvelles vulnérabilités

5.2 Recommandations à court terme

Les actions suivantes sont recommandées pour une mise en œuvre immédiate:

1. **Renforcement de la formation:**
2. Intégrer des scénarios de panne de communication dans les sessions de simulateur
3. Développer des aide-mémoires spécifiques pour les procédures de secours

Sensibiliser aux risques d'interférence et de brouillage

Amélioration des procédures:

6. Réviser les procédures de vérification des systèmes avant vol
7. Standardiser les réponses aux défaillances partielles

Clarifier les critères de décision pour l'utilisation des systèmes alternatifs

Maintenance ciblée:

10. Augmenter la fréquence d'inspection des connecteurs et câblages
11. Mettre en place un suivi spécifique des défauts intermittents
12. Vérifier systématiquement les performances des antennes

5.3 Recommandations à moyen terme

Pour une mise en œuvre dans les 6 à 12 mois:

1. **Améliorations techniques:**

2. Installer des filtres anti-interférence améliorés sur les systèmes VHF
3. Mettre à niveau les logiciels de gestion des communications

Améliorer l'intégration entre les différents systèmes de communication

Renforcement de la cybersécurité:

6. Développer des protocoles de détection des intrusions
7. Mettre en place des procédures de vérification des données ADS-B

Former le personnel technique aux menaces cybernétiques

Surveillance et reporting:

10. Créer un système dédié de reporting des anomalies de communication
11. Analyser systématiquement les tendances de défaillance
12. Partager les informations avec l'industrie et les autorités

5.4 Recommandations à long terme

Pour une mise en œuvre dans un délai de 1 à 3 ans:

1. **Évolution technologique:**

2. Évaluer l'intégration de nouvelles technologies de communication
3. Participer aux groupes de travail sur les standards futurs

Préparer la transition vers les communications basées sur IP

Recherche et développement:

6. Étudier les solutions d'authentification renforcée pour les communications
7. Développer des systèmes de détection automatique des anomalies
8. Explorer les technologies de communication quantique pour les applications critiques

6. PLAN D'ACTION

Le tableau ci-dessous présente le plan d'action proposé pour la mise en œuvre des recommandations:

Action	Priorité	Responsable	Échéance	Ressources requises
Formation simulateur	Haute	Chef instructeur	3 mois	Temps simulateur, matériel pédagogique
Révision procédures	Haute	Opérations aériennes	2 mois	Groupe de travail, documentation
Inspection ciblée	Moyenne	Maintenance	1 mois	Personnel technique, équipement test
Filtres anti-interférence	Moyenne	Ingénierie	6 mois	Budget équipement, temps d'immobilisation
Protocoles cybersécurité	Haute	IT/Sécurité	6 mois	Expertise externe, logiciels
Système de reporting	Moyenne	Qualité/Sécurité	4 mois	Développement logiciel, formation
Étude nouvelles technologies	Basse	R&D	18 mois	Budget recherche, partenariats

7. CONCLUSION

Cette analyse simplifiée de la sécurité des systèmes de communication aéronautique a permis d'identifier les principaux risques et de proposer des mesures d'atténuation adaptées. Les systèmes actuels offrent un niveau de sécurité satisfaisant grâce aux multiples redondances et aux procédures en place.

Cependant, l'évolution rapide des technologies et l'émergence de nouvelles menaces nécessitent une vigilance constante et une approche proactive. La mise en œuvre des recommandations formulées permettra de renforcer davantage la résilience des systèmes de communication face aux défaillances techniques et aux menaces externes.

La sécurité des communications aéronautiques est un élément fondamental de la sécurité des vols. Elle nécessite une collaboration étroite entre les opérateurs, les constructeurs, les fournisseurs de services et les autorités de régulation.

8. RÉFÉRENCES

- EASA CS-25.1431 "Electronic Equipment"
- EASA AMC 25.1309 "System Design and Analysis"
- FAA AC 120-76D "Authorization for Use of Electronic Flight Bags"
- FAA AC 20-140C "Guidelines for Design Approval of Aircraft Data Link Communication Systems"
- OACI Annexe 10 "Télécommunications aéronautiques"
- RTCA DO-178C "Software Considerations in Airborne Systems and Equipment Certification"
- RTCA DO-254 "Design Assurance Guidance for Airborne Electronic Hardware"

ANNEXES

- Annexe A: Glossaire des termes et abréviations
- Annexe B: Matrice détaillée d'évaluation des risques
- Annexe C: Statistiques d'incidents liés aux communications (2020-2025)
- Annexe D: Diagrammes des systèmes de communication

Ce document est conforme aux exigences de documentation technique définies par l'EASA Part-CAMO.A.200 et la FAA AC 120-92B.

DOCUMENT CONTRÔLÉ - RÉVISION 2.3

