Aircraft Security Process (Airbus)

Introduction et Contexte. — Processus de sécurisation des **AIS** (Aircraft Information Systems). Évolution vers l'ouverture des systèmes (**Open World**) et augmentation massive de la complexité logicielle (A320 ≈ 30 parts vs A350 ≈ 450 parts).

Technologies Avioniques. —

- **A320/A330 (Classique) :** Systèmes indépendants, bus **ARINC 429** (unidirectionnel, point à multipoint, 100 Kbps, 32 bits/label).
- **A380/A350 (Moderne) : IMA** (Integrated Modular Avionics). OS partitionné (**ARINC 653**) : cloisonnement spatial et temporel.
- **AFDX (Deterministic Ethernet) :** Basé sur des **VL** (Virtual Links). Commutation gérée par des switches qui imposent les routes. Bidirectionnel via deux VL.

Principes de Protection (Golden Rules). —

- **Défense en profondeur :** Accumulation de barrières pour ralentir l'attaquant.
- **Règle des 2 barrières :** Obligatoire pour les actifs à impact de sécurité **Strong/Very Strong**.
- **Zéro vulnérabilité commune :** Les barrières successives doivent utiliser des technologies différentes (ex : OS différents, COTS variés, Hardware vs Software).
- **Fail-Secure vs Fail-Safe :** En cas de panne, le système doit rester **sécurisé** (verrouillé), contrairement au Fail-Safe qui privilégie la sécurité immédiate des personnes (ouverture).
- **Absence de Bypass :** Aucune voie de contournement ne doit exister.
- **Signature numérique :** Garantie de l'origine et de l'intégrité du **FLS** (Field Loadable Software).

Mesures de Sécurité Techniques. —

- **Firewall (L3/L4) :** Filtre IP/Ports. Politique : "Drop everything, allow only what you need". Limite : ne protège pas contre les payloads malveillants sur les ports autorisés.
- **Application Level Gateway (ALG) :** Filtre les couches hautes (L7). Comprend les protocoles applicatifs. **Avantage :** Protection réelle de l'application. **Inconvénient :** Coût élevé, spécifique à chaque protocole.
- **VPN :** Assure intégrité, authenticité et confidentialité via tunnel crypto sur réseau hostile. Ne protège pas si l'attaquant est déjà dans le réseau de confiance.

Analyse de Risques et Menaces. —

- **Asymétrie :** L'attaquant cherche 1 faille ; le défenseur doit tout protéger.
- **Vecteurs :** USB, stations de maintenance, liaisons radio (SATCOM/WiFi), interfaces de chargement de données.
- **Types d'attaques :** Buffer overflow, DoS (flooding, épuisement de ressources), Spoofing, MitM, Jamming.
- **Points critiques :** Systèmes de monitoring/admin (accès total) et modes dégradés (souvent moins protégés).

Assurance et Certification (SAL). — Niveaux d'assurance (**SAL - Security Assurance Level**) :

- **SAL 0b :** Bonnes pratiques de développement, gestion vulnérabilités COTS.
- **SAL 1b :** Focus sur les fonctions de sécurité (SEF). **SAL 1 :** Tests Black Box.
- **SAL 2 :** Fonctions de support. Traçabilité complète. Tests **Grey Box**.
- **SAL 3 :** Composants interférents. Traçabilité design. Tests **White Box** (pénétration totale).

V&V et Tests de Pénétration (Pen-Tests). —

- **Vérification :** "La clé ouvre le verrou" (conformité aux specs).
- **Validation :** "La porte est bien fermée" (répond au besoin de sécurité).
- **Pen-Tests :** Obligatoires avant le **Type Certificate** (TC). Testent tous les chemins d'attaque depuis les interfaces externes. Réalisés par Airbus (1VV), auditeurs externes ou agences nationales.

Maintien en Conditions de Sécurité (MCS). — Processus cyclique post-livraison :

1. **Asset Inventory :** Création du **SBOM** (Software Bill of Material).
2. **Vulnerability Monitoring :** Veille NVD, CERTs, CVE.
3. **Assessment :** Scoring **CVSS** (Base, Temporal, Environmental).
4. **Decision/Treatment :** Patch immédiat, correction prochaine version, mitigation ou acceptation du risque.

Contraintes Spécifiques à l'Aéronautique. —

- **Cycles de vie :** 25 à 50 ans (obsolescence majeure).
- **Certification :** Processus long, fige les configurations.
- **Absence d'admin :** Pas de gestionnaire de sécurité humain à bord en temps réel.
- **Trade-offs :** Équilibre permanent entre **Sécurité**, **Coût** et **Usabilité**. La mesure technique doit toujours primer sur l'organisationnelle (procédure humaine).

I. Concepts Fondamentaux et Menaces. —

- **Dualité Sécurité :**
  - **Physique :** Protection contre l'accès humain non autorisé, dépôt d'explosifs, armes, illuminations laser (FAA simulations), drones et ManPADS.
  - **Cyber :** Protection contre les compromissions logicielles (virus/worms), dénis de service (DoS), et abus dirigés des systèmes IT embarqués.
- **Évolution du Risque :** Passage de systèmes **Simples/-Propriétaires/Isolés** à des systèmes **Complexes/-Standardisés/Connectés**.

- **Facteurs d'Exposition :** Utilisation massive de composants **GP-COTS** (General Public Commercial Off The Shelf), connectivité passagers accrue, et absence d'administrateur sécurité à bord.
- **Objectifs CIA : C**onfidentialité (sensibilité info), **I**ntégrité (info erronée non détectée/logiciel corrompu), **A**vailabilité (système réactif).
- **Cas d'Étude :** Hugo Teso (Planesploit via app mobile), Chris Roberts (connexion via boîtier IFE sous le siège).

II. Cadre Réglementaire et Autorités. —

- **OACI (ICAO) :** Créée par la Convention de Chicago (1944). Définit les standards **SARPs** (Annexes 1-18).
- **EASA / FAA :** Agences de certification. La réglementation est **Evolving** (évolutive) et parfois contradictoire.
- **Spécifications de Certification (CS) :**
  - **CS 25.795 :** Sécurité Physique (post-11/09).
  - **CS 25.1319 :** Sécurité Cyber (Protection contre les interactions électroniques intentionnelles non autorisées - IUEI).
- **Normes Clés :**
  - **ED202A / DO-326A :** Processus de sécurité.
  - **ED203A / DO-356A :** Méthodes et architecture.
  - **ED204 / DO-355 :** Navigabilité continue.
- **Approbations d'Organisme :**
  - **DOA (Design) :** Certifie la conception (Type Certificate).
  - **POA (Production) :** Garantit la conformité de fabrication (FAL, tests en vol).
  - **MOA / CAMO :** Maintien du niveau de sécurité en service.

III. Méthodologie Airbus de Gestion des Risques. —

- **Modèle de Risque : Risque = Consequence (Impact) × Likelihood (Probabilité).**
- **Composantes de l'Attaque :** Attaquant (Profil) → Point d'Entrée (Vecteur) → Vulnérabilité (Exploitation) → Asset (Cible).
- **Profils d'Attaquants (AP) :**
  - Malware non ciblé (bas impact).
  - Drive-by (Script kiddie, fun/opportunité).
  - Motivation commerciale (espionnage, crime organisé).
  - Terroriste / État (Agent national).
- **Likelihood (Vraisemblance) :** Dépend de la motivation, de l'**impunité** (anonymat), des moyens de préparation/exécution et de la fenêtre d'opportunité.
- **Impact Scales :** Catégories Sécurité (Catastrophique à Mineure), Opérations (Business), Image/Réputation.

IV. Design for Security (Principes de Défense). —

- **Défense en Profondeur :** Protection multicouche (barrières) pour ralentir et décourager l'attaquant.
- **Asymétrie :** L'attaquant n'a besoin que d'une faille ; le défenseur doit tout protéger.
- **Domaines de l'Avion (ARINC 664 p5) :**
  - **ACD (Aircraft Control Domain) :** Critique (Moteurs, vol, hydraulique). Zone **Closed**.
  - **AISD (Airline Info Services Domain) :** Support maintenance/équipage. Zone **Private**.
  - **PIESD (Passenger Info & Ent. Domain) :** IFE, Wi-Fi cabine. Zone **Public**.
  - **POD (Passenger Owned Devices) :** Appareils personnels, non contrôlés.
- **Hypothèses de Confiance :** Équipage et mainteneurs **Trusted** par défaut, mais leurs **e-tools** (laptops, USB, tablettes) sont **Untrusted**. Les signaux aéro (GPS, ILS) sont considérés comme non-sources de menace.

V. Processus Industriel et Cycle de Vie. —

- **Industrial Security :** Protection des usines, fournisseurs et lignes d'assemblage (FAL).
- **Objectifs Production :** Assurer que l'avion est **Free from malicious code** à la livraison et que les outils e-Tools n'altèrent pas les systèmes.
- **Maintenance Sécurisée :** Gestion des vulnérabilités via la **NVD** (National Vulnerability Database), audits de sécurité et surveillance des expirations de certificats.
- **Check-list Sécurité :** Formulaire obligatoire lors de toute modification de conception (CR/RFC) pour évaluer l'impact sur les barrières ou l'exposition des interfaces.

VI. Synthèse des Règles d'Or. —

- **Zéro Risque :** N'existe pas. L'objectif est l'acceptation du **risque résiduel**.
- **Anticipation :** Plus la sécurité est incluse tôt dans le cycle (V-cycle), moins elle est coûteuse.
- **SAL vs DAL :** Le DAL (Development Assurance Level) ne couvre pas la sécurité ; le **SAL** (Security Assurance Level) ajoute des exigences spécifiques contre les actes malveillants.
- **Discipline :** La sécurité contribue à la **Safety**, mais reste une discipline distincte avec des outils d'analyse dédiés (AFIA, AISAC).

Secu drones (Jean-Christophe Schiel)

Synthèse Drones : Missions, Télécoms & Propagation

I. Introduction et Missions. —

— **UAV Comms :** Liaisons de données (TC/TM), transmission de données de mission vers centre d'exploitation.

— **Usage Militaire/Sécurité :** Relais radio (portée/intervisibilité), nœud de comm aéroporté (cellulaire, maillé MANET, BACN).

— **Flux : Montant (Uplink)** = Télécommande (TC) ≈ kbps. **Descendant (Downlink)** = Télémesure (TM) ≈ kbps + Données mission (Mbps).

— **Localisation :** GPS (souvent contesté/spoofing), mode backup nécessaire.

— **Classif. Civile (DGAC) : Ouverte** (faible risque, déclaratif), **Spécifique** (SORA, STS/LUC), **Certifiée** (risque fort, licence pilote).

II. Types de Liaisons de Données. —

— **LOS (Line Of Sight) :** Visibilité directe. Haut débit (>300 Mbps), portée ≈ 300 km. Discret, résistant au brouillage.

— **BLOS (Beyond/Below LOS) :** Relais satellite. Portée illimitée, débit limité (Mbps). Sensible au brouillage, dépendance civile.

III. Propagation Radio - Formules Fondamentales. —

— **Loi en $1/r^2$:** La densité de puissance est inversement proportionnelle au carré de la distance.

— **FSPL (Free Space Path Loss) :** $FSPL = \left(\frac{4\pi df}{c}\right)^2 \implies FSPL_{dB} = 20\log_{10}(f_{MHz}) + 20\log_{10}(d_{km}) + 32,44$.

— **Équation de Friis :** $P_r = P_e \cdot G_e \cdot G_r \cdot \left(\frac{\lambda}{4\pi r}\right)^2$.

— **Bilan de liaison (dB) :** $P_r = P_t + G_t + G_r - FSPL - P_{pertes}$.

— **Pertes P1 (Physiques) :** Absorption, diffraction, réflexions multiples, masquage.

— **Pertes P2 (Système) :** Câbles, connectique, désadaptation d'antenne.

IV. Zones de Rayonnement et Obstacles. —

— **Zones :** Rayleigh (proche, quasi-constante), Fresnel (fluctuante), Fraunhoffer (loi en $1/r$).

— **Horizon Géométrique :** $d_m \approx \sqrt{2R_t}(\sqrt{h_1} + \sqrt{h_2})$.

— **Ellipsoïde de Fresnel :** Condition LOS = 60% du 1er ellipsoïde dégagé. Rayon $R_f = \sqrt{\frac{\lambda d_1 d_2}{d_1 + d_2}}$.

— **Diffraction :** Principe de Huygens (chaque point devient source). Effet de pointe si $R_0 \approx 0$.

V. Facteurs d'Atténuation Environnementaux. —

— **Polarisation :** Perte $P_{polar} = -20\log(\cos\theta)$. Ex : 20° permet -0,5 dB.

— **Atmosphère :** Absorption moléculaire (H_2O, O_2). Pics d'atténuation selon fréquence (ex : 22 GHz, 60 GHz).

— **Hydrométéores :** Atténuation linéique (dB/km) augmente drastiquement avec l'intensité de la pluie (mm/h) et la fréquence (>10 GHz).

— **Effet Doppler :** Décalage fréquentiel $\Delta f = \frac{\Delta v}{c} f_0$.

VI. Chaîne Télécom (Architecture). —

— **Source Formatting :** Conversion analogique/numérique (bits).

— **Source Coding :** Compression des données.

— **Encryption :** Sécurisation (Optionnel).

— **Channel Coding :** Correction d'erreurs (FEC).

— **Modulation :** DSSS (étalement spectre), FHSS (sauts de fréquence) pour protection brouillage.

— **Adaptation :** Amplification et antenne.

Synthèse Sécurisation Communications Drones

Chaîne de Transmission. —

— **Source Coding** : Réduit débit. **Lossless** (Winzip, 7Zip) vs **Lossy** (MP3, H264/H265).

— **Chiffrement** : Rend l'info illisible (AES 256 bits, SSL).

— **Channel Coding** : Ajoute redondance vs bruit. **Hamming** (bloc, correction 1 bit), **Convolutionnel** (Viterbi), **Turbo-codes** (limite de Shannon).

Modulation & Accès. —

— **Types** : **FSK** (Fréquences), **ASK** (Amplitudes), **PSK** (Phases : BPSK, QPSK), **QAM** (Mixte : 16QAM, 64QAM).

— **Efficacité** : QPSK (2 bits/symb), 16QAM (4 bits/symb), 64QAM (6 bits/symb).

— **Duplexing** : **FDD** (2 fréquences UL/DL), **TDD** (partage temporel).

— **Accès Multiple** : **FDMA** (Fréquence), **TDMA** (Temps), **CDMA/WCDMA** (Code), **OFDM** (Multi-porteuses orthogonales).

Adaptation au Médium & Bilan de Liaison. —

— **Conversion RF** : Modulateur quadrature (I/Q), Amplis (PA, LNA), Antennes.

— **Indicateurs** : **BER** (Taux d'erreur binaire), **SNR** (Signal/Bruit), **SINR** (Signal/Interférence+Bruit), **EVM** (Error Vector Magnitude).

— **Link Budget** : $P_r = P_e - L_e + G_e - L_p + G_r - L_r$. Condition : $P_r > N + I + SNR_{min} + M$.

Fréquences & Normalisation. —

- **Bandes UAV** : **L** (1-2 GHz), **S** (2-4 GHz), **C** (4-8 GHz), **X** (8-12 GHz), **Ku** (12-18 GHz).
- **Réglementation (France)** : Bande **X interdite** ; **Ku (14,5-15,25 GHz) autorisée**.
- **Drones Civils** : ISM 2,4 GHz & 5,5 GHz. Études sur 4G/5G.
- **STANAG 7085** : Standard OTAN (Liaison de données). **CDL** (USA : OQPSK + Reed Solomon) vs **DVBS** (FR : QPSK + Viterbi). Incompatibles entre eux.
- **STANAG 4586** : Architecture drone et charges utiles.

Tendances & Modems. —

- **Évolutions** : Réutilisation stack IP civil, interopérabilité Niveau 3 (Réseau).
- **Protocoles** : **MAVlink** (Open-source), **DSMX** (Loisir).

Synthèse : Sécurisation des Communications Drones

1. Architecture & Modems. —

- **Modèles Modems :**
  - **Silvus (MN-MIMO) :** 85 Mbps UDP, latence 7ms, C-OFDM, AES 128/256 bits, IP67.
  - **Hypercable (HYC-540) :** 12 Mbps, COFDM TDD, Full Duplex (Vidéo HD/Data), durci.
  - **Simpulse :** 10 kbps à 10 Mbps, interfaces Ethernet/USB/Série, poids 97g-130g.
- **Architecture Fonctionnelle :** Divisée en 3 couches : **Perception** (Comms/Capteurs), **Controller** (Flight Control), **Decision** (Guidage/Navigation).
- **UAM (Urban Air Mobility) :** Niveaux d'autonomie FAA (ACLs) de 0 à 5.
  - **HWTL :** Human-within-the-Loop (Manuel).
  - **HOTL :** Human-on-the-Loop (Surveillance).
  - **HOVTL :** Human-over-the-Loop (Haute autonomie).
- **Standards Militaires :** Utilisation des protocoles **STANAG** (4586 pour UCS, 7085 pour Data Link, 4545 pour Payload).

2. Menaces & Lutte Anti-Drone. —

- **Cyber :** Attaques sur liens IP (surtout via réseaux 3G/4G/5G), interception de flux vidéo non chiffrés.
- **Radio :**
  - **Brouillage (Jamming) :** Rupture du lien sol-bord.
  - **Spoofing :** Usurpation de coordonnées satellite (GPS L1, GAL E1, GLO L1) pour dévier le drone.
- **Stratégies de défense :**
  - **Physique :** Lasers (HELMA-P), micro-ondes haute puissance (THOR), fusils de précision.
  - **Électronique :** Brouilleurs directionnels, systèmes de détection acoustique/radar.

3. Sécurisation : Moyens & Techniques. —

- **Sécurisation Réseau :** Durcissement des OS (Hardening), authentification forte, gestion des droits (Télépilote vs Technicien vs Administrateur), isolation des interfaces.
- **Sécurisation Radio (TRANSEC & COMSEC) :**
  - **LPI/LPD :** Low Probability of Intercept/Detection.
  - **FHSS :** Sauts de fréquence aléatoires (contre les effacements).
  - **DSSS :** Étalement par séquence directe (optimise le gain système).
  - **Hybride :** Combinaison FHSS/DSSS pour une résistance maximale.
- **AJM (Anti-Jamming Margin) :** Rapport Puissance brouilleur / Puissance liaison.
- **Futur Optique :**
  - **FSL (Free Space Laser) :** Débit 1 Gbps, quasi-impossible à intercepter.
  - **QKD :** Sécurisation par distribution quantique de clés.
  - **Filaire :** Utilisation de fibres optiques (portée 70km+) pour une immunité totale aux RF.

4. Paramètres de Performance (MIL). —

- **Disponibilité temporelle :** $> 99\%$ (TC/TM), $> 90\%$ (Data).
- **Précision de localisation :** Distance < 20m, Angle < 5 mrad.
- **Niveaux de protection :**
  - **Niveau 1 :** Comportement prédictible sous brouillage.
  - **Niveau 2 :** Protection intégrée dès la conception.

Présentation du métier d'intégrateur (Aurélien Bouzon)

I. LE MÉTIER D'INTÉGRATEUR & ÉCOSYSTÈME

Sociétés de Services (ESN/SSII). —

— **Gammes :** Conseil/Assistance, Intégration, Infogérance.

— **Acteurs majeurs :** Capgemini, Atos, IBM, Accenture, Sopra Steria, Orange Business (OBS).

— **Certifications (Reconnaissance pro) :** CISSP (Pro), CISA (Auditeur), CISM (Manager), CEH (Hacker éthique), ISO 27001 Lead Auditor.

Rôle de l'Intégrateur. —

— **Mission :** Sélectionner et assembler des briques (SW/HW) pour répondre à un besoin.

— **Phases (Cycle en V) :** Recueil besoin → Proposition → Développement/Intégration → Test/Validation → Déploiement → Support.

— **Livrables :** Cahier des charges, études de faisabilité, Dossier d'Architecture (DAG), Dossier de Recette (DEX), manuels d'installation.

— **Contrainte :** Documentation souvent plus conséquente que le produit fini.

II. AVIATION CIVILE : ORGANISATION & SYSTÈMES

Structure DGAC. —

— **Tutelle :** Ministère de l'Écologie (MEDDE).

— **DSNA (Prestataire) :** Fournit les services de contrôle aérien. Partenaires : Eurocontrol, Air France, Météo France, Armée.

— **DTI (Technique) :** Définit, réalise et installe les systèmes (Radar, Radio, Réseaux).

Systèmes Techniques. —

— **Radars :** Primaire (écho), Secondaire (transpondeur), Multilatération.

— **Aides pilotage :** VOR, DME, ILS.

— **Réseau RENAR IP :** Réseau national maillé sécurisé (remplace X25), évite les SPOF (*Single Point of Failure*).

— **Évolution :** Passage du papier (strips) au numérique (Projet 4Flight).

III. ENJEUX DE SÉCURITÉ ET RÉGLEMENTATION

Contexte d'ouverture. —

— **Menaces :** Passage d'un monde fermé à un monde connecté (Internet, ADS-B vulnérable à la corruption de données, Wifi/Satcom en vol).

— **Critères DIC :**

  — **Disponibilité :** Critique (H24).

  — **Intégrité :** Priorité absolue (données radar/plan de vol).

  — **Confidentialité :** Faible (données souvent publiques).

  — **Authenticité :** Cruciale mais difficile sur les ondes radio.

Cadre Légal. —

— **OIV (Opérateur d'Importance Vitale) :** Activité dont l'arrêt mettrait en cause la survie de la Nation ou la vie de la population.

— **LPM (Loi de Programmation Militaire) :** Obligations de notifier l'ANSSI, audits réguliers, isolation des systèmes critiques.

— **ANSSI :** Rôle de conseil, surveillance, audit et qualification du matériel.

IV. ARCHITECTURE RÉSEAU SÉCURISÉE

Concepts de Défense. —

— **Sécurité Périmétrique :** Modèle concentrique avec Pare-feu (FW). Le maillon le plus faible définit le niveau global.

— **Défense en Profondeur :** Sécurisation de toutes les couches OSI. Observation et détection à chaque étage.

— **Sécurité Physique :** Fondement de tout SI (Contrôle d'accès, Multi-facteur : Ce que je sais/suis/possède).

Principes de base. —

— **Moindre privilège :** Tout ce qui n'est pas autorisé est interdit.

— **Segmentation :** Éviter les réseaux à plat, isoler les fonctions critiques.

— **Anti-SPOF :** Redondance matérielle et électrique.

Outils Techniques. —

— **Réseau :** VLAN, Port Security, Routage statique, VPN.

— **Analyse :** IDS/IPS, DPI (Deep Packet Inspection), Sandbox, Honeypot.

— **Gestion :** SIEM/SOAR, EDR/XDR, Bastion, NTP.

— **Pare-feu (Marché) :** Fortinet, Cisco, Palo Alto, Check Point, Stormshield (français).

V. CAS PRATIQUE : DÉPOSE DE PLAN DE VOL

— **Besoins :** Interface Internet ↔ DMZ ↔ Réseau Partenaire.

— **Mesures :** NAT (masquage IP), filtrage par matrice de flux (connexions stateful), segmentation stricte.

— **UTM/USM :** Appliances combinant FW, Antivirus, Proxy, et IPS (attention au SPOF fonctionnel).

VI. Cas d'Application : Sécurité & Infrastructure

1. Filtrage Applicatif (L7). —

— **Objectifs :** Autoriser uniquement requêtes bien formées ; filtrage via machine dédiée (**Proxy**) en zone **Bastion**.

— **WAF vs SWG :** WAF = reverse proxy (protection serveur) ≠ SWG = proxy (protection utilisateur).

— **Techniques :** Filtrage URL/paramètres via **REGEX** (Whitelist/Blacklist).

— **Protocoles :** Web (HTTP), mais aussi SNMP, SYSLOG, NTP, FTP. Protocoles non-standards → dév spécifique.

2. Réplication & Disponibilité. —

— **Besoins :** Empêcher compromission plans de vol ; modération ; zone spécifique (**Réplique**).

— **Taux de service (SLA) :**

— **99,99%** (∼1h/an) : Remplacement matériel à froid.

— **99,999%** (∼5min/an) : Remplacement matériel à chaud (redondance complète).

— **Haute Disponibilité (HA) :**

— **Actif/Passif :** 1 seule unité transfère la donnée.

— **Actif/Actif :** Loadbalancing entre plusieurs unités.

— **Mécanisme :** @IP et @MAC virtuelles ; protocoles VRRP, HSRP, CARP, Heartbeat.

— **Risque Split Brain :** 2 unités actives simultanément (conflit IP/MAC). Solution : liens HA doublés et identifiés.

3. Virtualisation & Conteneurisation. —

— **Avantages :** Économique, modulaire, restauration/reprise rapide, allocation dynamique.

— **Inconvénients :** Point de défaillance commun (nécessite double hyperviseur), surface d'attaque accrue (code sup.), administration complexe.

4. Protection DoS & Détection d'Intrusion. —

— **Anti-DDoS :** Limiter nb connexions par IP/semi-ouvertes ; mise en cache proxy ; DNS balancing ; duplication de site.

— **SIEM (Security Information Event Management) :** Collecter (Syslog/SNMP), Archiver, Normaliser (Parsers), Corréler (alertes), Reporter.

— **SOAR :** Automatisation de l'analyse et réponse pour réduire la vitesse de propagation.

— **Supervision (SNMP) :** v1/v2 (clair), v3 (Authenticité/Confidentialité AES/Intégrité SHA). Préférer le **Polling** (UDP/161) au **Trap** (UDP/162) car plus fiable en cas de congestion ou panne électrique.

5. Terminologie EDR/NDR. —

— **Système : AV** (signatures) → **HIDS** (comportemental) → **EPP** (politique sécurité) → **EDR** (télémétrie détaillée).

— **Réseau : IDS** (détection seule) → **IPS** (bloquant) → **NTA/NDR** (analyse flux/réponse). Efficacité max sur flux non chiffrés.

VII. Durcissement Système (Hardening)

Principes de base. —

— **Réduction surface d'attaque :** Code minimal ("présent uniquement si nécessaire").

— **Gestion Utilisateurs :** Privation de shell, groupes restreints, complexité/durée de vie MDP (cracklib), **MFA**, interdiction login **root** direct.

— **Services :** Bannissement (échecs répétés), limiter visibilité version/bannières, limiter services bavards (Avahi, Netbios), rotation logs (logrotate).

— **Réseau :** TCP Wrapper, ARP/Routage statiques, sysctl.

Contrôle d'Intégrité. —

— **Objectif :** Détecter modifications (Somme contrôle, Inode, Droits).

— **Fonctionnement :** 1. Générer base de référence à l'install (lieu sûr). 2. Analyse régulière vs référence.

— **Outils :** AIDE, Tripwire, CNAPP (Conteneurs).

VIII. Intégration & Conclusion

Automatisation. —

— **Outils :** Preseed/Kickstart (Install OS), Ansible/Puppet/Chef (Config/Idempotence).

— **Diversité :** Évite les SPOF et remédie aux 0-day, mais coûteux en formation/maintenance.

Cycle de vie de l'attaque. —

— **Avant :** Architecture, PRA/DRP, Audit, Sensibilisation.

— **Pendant :** Détection (SOC/SIEM), Limitation impacts, Confinement.

— **Après :** Forensic (retrouver l'attaquant), Reprise activité, Apprentissage.

Axiomes de sécurité. —

— **Stoïcisme :** Le défenseur a plus à perdre ; il est plus facile de détruire que de construire.

— **Facteur Humain :** "No patch for human stupidity" → Seul vaccin : formation ingénierie sociale.

— **Équilibre :** Sécurité / Fonctionnalité / Facilité d'utilisation.

Secu communication aérospatiales (Benoît Tranier)

1. Fondamentaux SSI & Cryptographie

- **Principes (CIA) : Confidentialité** (accès restreint), **Authenticité** (source avérée + intégrité du message), **Disponibilité** (accès 24/7, assurée par redondance physique).
- **Analyse Statistique :** Les langages ont des signatures (ex : fréquences de lettres). Une crypto faible (César) n'efface pas ces traces. Une crypto forte produit un message indiscernable d'un **aléa statistique**.
- **Principe de Kerckhoffs :** La sécurité repose sur le secret de la **clé** uniquement, pas sur l'algorithme.
- **Complexité :** Un système est sûr si le déchiffrement nécessite une puissance de calcul déraisonnable.
- **Évolutions :** Transition vers le **Post-Quantique** (PQC) et la distribution quantique de clés (QKD). Durée de validité des certificats en forte baisse (passant de 84 à 13 mois).

2. Architecture des Systèmes Spatiaux

- **Segments :**
  - **Satellite :** Plateforme (vie/orbite) + Charge Utile (mission).
  - **Sol (GCC) :** Contrôle (maintien à poste, TM/TC).
  - **Mission (MCC) :** Interface utilisateur et config charge utile.
  - **Utilisateur :** Bénéficiaires finaux (Gateways, terminaux).
- **Liens vitaux : TM/TC** (Télémesure/Télécommande) = "Fil d'Ariane". Si rompu, satellite perdu.
- **Canaux TM/TC : Primary Link** (haut débit, directionnel, mode nominal) et **Secondary Link** (bas débit, omnidirectionnel, mode survie/LEOP).

3. Orbitographie & Missions

- **LEO (200-2000 km) :** Obs. Terre (SSO), constellations (Starlink). Latence < 100ms. Durée de vie : 5-10 ans. **OBP** (On-Board Processor) type routeur IP.
- **MEO (∼20 000 km) :** Navigation (GPS, Galileo, Beidou, Glonass). Durée de vie : ∼12 ans.
- **GEO (35 786 km) :** Télécom fixes, météo. Latence > 500ms. Pas de couverture des pôles (>80°). Durée de vie : 15-20 ans. **DTP** (Digital Transparent Processor) type répéteur.
- **HEO :** Orbites elliptiques (Molnya) pour zones polaires.

4. Typologies de Missions Télécom

- **ComSatCom :** Civil, bonne disponibilité (ex : Konnect).
- **GovSatCom :** Critique/Secours, forte disponibilité (ex : Athena-Fidus).
- **MilSatCom :** Militaire, disponibilité maximale (ex : Syracuse).
- **LEO PNT :** Nouveau concept visant à améliorer la précision/dispo de la navigation MEO.

5. Cycle de Vie & Enjeux

- **Phases : LEOP** (Transfert vers orbite finale), **IOT** (Tests en orbite), **OCO** (Opérations nominales), **EOL** (Fin de vie).
- **Fin de vie :** Désorbitation vers atmosphère (LEO) ou envoi en **orbite cimetière** (+300 km) avec passivation (GEO).
- **Méga-constellations :** Enjeux de renouvellement (ex : 8400 lancements/an pour maintenir 42 000 satellites), gestion des débris et ressources en métaux rares.

1. Concepts Fondamentaux & Sémantique

- **Flux :** Ensemble des données distribuées d'un point A vers un point B.
- **Canal / Lien :** Chemin physique (ex : bande de fréquence RF) acheminant le flux.
- **Importance :** Les mécanismes de protection diffèrent selon qu'ils ciblent le flux (données) ou le canal (chemin).

2. Typologie des Flux Spatiaux

- **TM/TC :** Télémesures (état satellite) et Télécommandes (actions/config). Présence **obligatoire** sur tout satellite.
- **AOS (Advanced Orbiting System) :** Données missions (images, mesures). Flux montant rare (ex : ISS audio/vidéo).
- **Autres :** Liens inter-satellites (ISL), mesures de distance (non protégées), flux IP (satellites LEO type Starlink).

3. Standards et Modèle de Couches

- **Organismes : CCSDS** (International) et **ECSS** (Européen, souvent dérivé du CCSDS).
- **Modèle CCSDS/ECSS vs OSI :** La couche **Liaison** spatiale est plus riche ; elle intègre la QoS (retransmission) normalement propre au Transport (TCP) en OSI.
- **Structure des couches :** Physique → Codage (BCH, Reed Solomon) → Transfert (ID satellite, intégrité) → Paquet (ID processus bord).

4. Sécurité : Le Standard SDLS (Space Data Link Security)

- **Services COMSEC :**
  - **Confidentialité :** Chiffrement des paquets (données missions).
  - **Authenticité/Intégrité :** Protection des trames jusqu'au niveau transfert.
- **Ordre de vérification :** 1. Intégrité de transmission (CRC du Trailer) → 2. Authenticité/Intégrité cryptographique (MAC de sécurité).
- **Security Association (SA) :** Paramètres et algorithmes négociés. Souvent simplifié en spatial (une seule primitive).

5. Analyse de Risque et Menaces

- **Motivations :** Financières (indisponibilité = millions d'€/mois), espionnage, sabotage (désorbitation), image de marque.
- **Types d'attaques :**
  - **Rejeu (Uplink TC) :** Enregistrement et réémission de commandes valides. **Parade :** Compteur d'Anti-Rejeu (CAR) incrémental et authentifié.
  - **Brouillage (Jamming) :** DoS sur lien montant ou descendant. Peut mener à la perte du satellite.
  - **Attaque Indirecte :** Prise de contrôle d'un satellite tiers mal protégé pour l'utiliser comme "impacteur" contre une cible.
- **Points faibles :** Les stations sol (TCR/Gateways) sont souvent moins protégées que le Centre de Contrôle (SCC).

6. Objectifs de Sécurité par Service

- **COMSEC (Liaison) :** Chiffrement (Confidentialité) + Authentification (Authenticité, Intégrité, Anti-rejeu).
- **TRANSEC (Physique) :** Disponibilité (anti-brouillage). Très complexe et coûteux, pas de standard établi.
- **EBIOS RM :** Méthode ANSSI utilisée pour identifier les biens essentiels et les objectifs de sécurité.

7. Implémentation Cryptographique

- **Conf. #1 (Intégrée) :** Logicielle (OBSW), privilégiée pour le civil.
- **Conf. #3 (HSM) :** Coupure physique matérielle, privilégiée pour le militaire/étatique.
- **Algorithmes :** Utilisation historique d'**AES ECB** séquencé (avec constantes/compteurs) pour la simplicité, bien que gourmand en bande passante. Transition vers **AES CTR** ou GCM.

1. COMSEC & Cryptographie TM/TC

CDU (Command Deciphering Unit). — Équipement de déchiffrement des télécommandes.

- **Mode :** Supporte AES ECB.
- **Historique :** Développé en 2005 (TurkSat 3A), encore utilisé sur Thor8/JSat32 (lancements 2027).
- **Architecture :** Comprend une tranche nominale et une tranche redondante.

Mode AES-GCM (NIST SP800-38D). — Utilisé pour les missions civiles/commerciales et la sécurisation https.

- **Séquencement :** AES en mode compteur (GCTR) car inadapté au flux continu brut.
- **Contrainte IV/Clé :** Probabilité de collision (IV, K) doit être $< 2^{-32}$. Ne jamais réutiliser un couple IV/Clé (risque de remonter à la clé).
- **Structure :** Inclut des données claires (*Additional Authenticated Data* - AAD), des données chiffrées, et un **TAG** (MAC) pour l'authenticité.

2. TRANSEC (Sécurité des Transmissions)

Protection contre les brouilleurs RF (militaires uniquement).

- **DSSS :** Étalement du signal par convolution avec une séquence pseudo-aléatoire sur un large spectre.
- **FHSS :** Sauts de fréquence du signal modulé.
- **Générateurs :** Séquences pilotées par algorithmes à clé secrète symétrique.
- **Complexité :** Impact lourd sur l'architecture bord-sol (modulateurs/démodulateurs spécifiques).

3. Menaces Spécifiques & Rayonnements

Rayonnements compromettants (TEMPEST). — Fuite d'info claire via couplage électromagnétique sur un signal chiffré.

- **Norme OTAN SDIP-27 :** Level A (1m), Level B (20m), Level C (100m).

Menaces Avérées. —

- **Viasat (2022) :** Malware "Acidrain" (wiper) via centre de gestion au sol (Turin). Impact : modems HS.
- **Skynet-1A :** Dérive inexpliquée. TC obsolètes (sans protection), prise de contrôle probable.
- **Loutch-Olimp-K (1 & 2) :** Satellites russes "butineurs" pour écoute passive et brouillage en orbite GEO.

4. Certification de Sécurité

Processus gérés par agences nationales (ANSSI, NSA, BSI).

- **Critères Communs (CC) :** Niveaux EAL 1 à 7. France : EAL3+ / EAL4+.
- **FIPS 140-3 :** Standard nord-américain (4 niveaux).
- **TOE (Target Of Evaluation) :** Périmètre physique évalué.
- **Documents :** ST (*Security Target*) rédigée par le soumissionnaire.

5. IGC (Infrastructure de Gestion de Clé)

SKI (Secret Key Infrastructure). — Basée sur des clés symétriques.

- **Mécanisme :** *Key Wrapping* (chiffrement de clé par une KEK).
- **Limites :** Difficile pour les constellations (N flux = $N(N-1)/2$ clés).
- **Règle :** Une clé est mieux protégée quand elle n'existe pas encore (génération à la volée).

PKI (Public Key Infrastructure). — Basée sur cryptographie asymétrique (RSA, DH).

- **Entités :** CA (Autorité de Certification), RA (Enregistrement), CMS (Annuaire/CRL).
- **Avantages :** Passage à l'échelle ($2N$ clés pour N utilisateurs).
- **Persistance du Secret :** *Forward Secrecy* (FS) via renouvellement de clés de session.
- **Authentification Spatiale :** Utilisation possible des **éphémérides** (position/vitesse) pour authentifier le satellite sans clé privée persistante.

6. Cycle de Vie des Clés

1. **Génération :** Aléa vrai, non prédictible.
2. **Affectation :** Identifiant unique, un seul service.
3. **Distribution :** Sécurisée (confidentialité/intégrité).
4. **Utilisation :** Respect des standards (ex : AES-GCM).
5. **Retrait :** Effacement définitif des clés "usées".

Gestion des Clés et Cryptopériode

Standards :. — NIST (SP800-57, 133, 135, 22), CCSDS 350.6-G-1, RGS Annexe B2 (ANSSI).

Dérivation :. — Utilisation d'une **clé maître** pour générer des clés de confidentialité/intégrité via un IV (*Initialisation Vector*).

Cryptopériode (Durée de vie max) :. — Influencée par :

- Taille de clé (résistance aux attaques exhaustives).
- Période des générateurs de pseudo-aléas.
- Mode d'opération (ex : AES $\leq 2^{64}$ appels par clé, ANSSI recommande 2^{48}).
- Unicité du couple IV/Clé et taille du compteur anti-rejeu.
- Débits des flux et criticité en cas de compromission.

Fréquences de renouvellement :. — Satellite (1 mois), TLS (chaque session), Asymétrique (1 an).

Service OTAR (Over The Air Rekeying) :. — Indispensable pour le renouvellement en vol (compromission sol, corruption bord, besoin de clés "fraîches").

Infrastructures de Gestion des Clés (IGC/PKI)

Modèle Client-Serveur vs Spatial :. —

- **Sol :** Sessions éphémères, bidirectionnelles (Full Duplex), effacement des secrets post-session.
- **Spatial :** Architecture complexe, sessions pouvant durer 20 ans (GEO), contraintes de calcul (historiquement limitées).

Topologie des Canaux (Exemple Satellite + 4 GSU) :. —

- **Télécommandes (TC) :** Mode "Point à Point". 8 clés secrètes nécessaires (2 SSU bord × 4 GSU sol). Chaque GSU a sa propre clé par SSU.
- **Télémesures (TM) :** Mode "Broadcast". 2 clés seulement (1 par SSU). Le satellite descend un flux unique, déchiffrable par tous les GSU simultanément.

Génération d'Aléas (TRNG/DRNG)

Menace :. — Attaques par **canaux cachés** (*side channel*) et prédictibilité. Un code JJ/MM (365 combinaisons) est 27x plus rapide à casser qu'un 4 digits aléatoire (10 000).

Structure d'un Générateur :. — Phénomène physique → Numérisation (**Aléas bruts**) → Post-traitement (**Pseudo-aléas**) → Évaluation statistique.

Types de RNG :. — Analogiques (chaotiques), Numériques (compteurs asynchrones), **Quantiques (QRNG)** (basés sur l'imprédictibilité de la mécanique quantique).

Standards de test :. — FIPS 140-2 (Poker, Monobit, Runs), AIS31 (recommandé Critères Communs), NIST SP 800-22 (15 tests dont Spectral, Matrix rank).

Règle d'or :. — **Ne jamais tester les aléas utilisés comme clés** (biaise l'entropie). Utiliser des flux dédiés aux tests.

Menace Quantique et Solutions

Impacts :. —

- **Algorithme de Shor :** Casse la cryptographie asymétrique (RSA, DH, ECC).
- **Algorithme de Grover :** Affaiblit la cryptographie symétrique (divise la sécurité par 2 → passer à AES-256).
- **Store-now-decrypt-later :** Collecte de données actuelle pour déchiffrement futur.

Cryptographie Post-Quantique (PQC) :. — Compétition NIST (2017-2024). Familles : Réseaux euclidiens (*Lattices*), Codes, Multivariée, Isogénies (ex : SIKE, cassé en 2022).

Hybridation :. — Recommandation ANSSI. Combiner ancien (sûr aujourd'hui) + nouveau (PQC) pour une défense en profondeur.

Distribution de Clés Quantiques (QKD) :. —

- **Principe :** Échange de photons polarisés. Toute mesure par un espion altère l'état (décelable).
- **Limites :** Portée fibre ≈ 100 km, coût élevé.
- **Spatial :** Satellite comme "nœud de confiance" (ex : satellite chinois Micius) pour relier des stations distantes (Graz-Xinglong, 7600 km).

Purpose of the Safety is to protect only people in the Aircraft ? Non, le but est aussi de protéger les gens au sol (d'un crash eventuel par ex.).
What is the difference between Safety and Security ? safety : pas malveillantant (accident), security : actes malicieux
Security is based on probability ? non, sur potentialité
What is a CRI ? SC ? CARI ? CS ? Certification Review Item, Special Conditions, Continuous Airworthiness Review Item, Certification Specification
What are some of the Security Principles ? security in depth(slow down attacker), global vision (prevent bypass), asymmetry (l'attaquant n'a besoin que d'1 faille, le défenseur doit tout défendre)
What means DOA, POA, MOA ? Design Organization Approval, Production Organization Approval, Type Certificate Holder(Maintain Security level)
What are the Domains considered in security ? ACD(Aircraft Control Domain), AISD (Airline Information Services Domain - info, opérationnel), PIESD (passager et entertainment)
What is the V&V main idea ? avion, systeme équipement, supplier, on reconfirme au niveau avion —-> pas sûr de la prise de note
What is the purpose of the Checklist ? Le but est de trier si y'a une activité ou non à faire en sécurité, si ça touche une barrière de sécu. Eviter d'avoir a repasser l'entièreté des trucs de sécu.
What means CIA ? Confidentiality, Integrity et Availability
What is the differences between SG, SM, SB ? segurity goal, security mesure, security barrier
What means EP ? AP ? Entry Point, Attacker Profile
What is an Impact ? $impact = threat + vuln$
What is a Risk ? $risque = impact + likelyhood$ (likelyhood = probabilité)
What is a TC ? TS ? Threat Condition, Threat scenario
What are some of the Golden Rules ? security assurance, resilience avion après incident, de de faille dans le code (à la livraison de l'avion par airbus), minimum 2 barrière de sécurité, aucune vulnérabilité n'affecte les 2 barrières, les barrières doivent être fail-secure
What is the principle of layer of defense ? Defense en profondeur ("c'est bien de mettre un impact et que le chien montent la garde")
What means SAR and SAL ? Security Assurance Requirement et Security Assurance Level

etendre portée LOS : augmenter taille antenne au niveau sol, augmenter hauteur du mat d'antenne (horizon)
étendre portée LOS (archi) : 4F/5G, interco SATCOM, LOS capable de maillage réseau
LOS 2.4GHz vs SATCIM 34GHz : rebond et multi trajets vont impacter le lien LOS, notion de dégagement de l'ellipsoide de Fresnel est plus contraignante que la LOS.
Spec moderne : AES256, coded OFDM
TRANSEC : brouilleur intelligent peut deviner le saut, une antenne directionnel peut offrir protection TRANSEC.
Moyen de protection drône civil : fréquence spécifique, multi-connectivité, lien optique
Sécurité des communication : CIA (Confidentialité, Integrité, Availability)
SCC (Centre Controle Satellite) : maintenir satellite sur orbite et surveiller systeme vitaux
CCSDS-SDLS (Space Data Link Security) : Confident., Int., Auth (pas CIA !)
précautions éléments sensibles : les aléa utilisés ne doivent pas être testé statistiquement mais la fonction de génération doit etre testé.
SKI & PKI : Secret Key Infrastructure (pas asymetrique) /Public Key Infrastructure(asymetrique), les 2 permettent l'échangent de clé symétrique.
QKD : Quantum Key Distribution, outrepasser la limite des 100km au sol
DICT : Disponilité, Intégrité, confidentialité et preuve(Traçabilité - non répudiation)
Taux de dispo (vrai) : 99,999% reprise automatique (car moins de 5min de downtime par an). taux elevé => peu d'interruption (car moins de down time)
SpOF (Single Point Of Failure) : peut être une source d'énergie, pas un problème si peu de dispo attendu.
VRRP (Virtual Router Redondancy Protocol : permet de définir une @IP relogeable au sein d'un groupe.
Segmentation rzo : limite que les risques se propagent, matos filtrant (firewalln VLAN), base de la sécu perimetrique
Hugo Teso : appli mobile qui récupère plan de vol et altitude... Sur simulateur. Après ça l'aviation a réagit avec ACARS.
Sécu obscurité naze ? peu couteut le reverse, confidentialité long terme complexe, prise en compte de leaks et insiders.
TC holder : maintenir niveau de sécu pendant opérations commerciales.
FLS (Field Loadable Soft) : certificats + changer sans outils
durée de vie d'un avion prévu : 25-50ans
verif vs valid/pentest : "la porte s'ouvre" vs "est-il possible de crocheter la serrure"
IMA (Integrated Modular Avionics) : A380/A350, utilise ARINC 653, permet positionnement spaci temporelle app.
Secu organisationelle : procédure opérationelle et mesure qui transforme la responsabilité vers les op

LEO vs GEO : LEO est désintégré, GEO est lancé vers un puit gravitationelle