# TLS-SEC

**Introduction au concept de « security » dans le domaine aéronautique**

ECOLE NATIONALE DE L'AVIATION CIVILE

SINA Department
TELECOM lab

**Nicolas LARRIEU**

Nicolas.Larrieu@ENAC.fr (room Z 157)

Décembre 2016

## Objectifs de cet enseignement

- ***Comprendre la différence entre la sécurité et la sureté dans un contexte général***
- ***Dans le contexte aéronautique, illustrer les recouvrements qui existent entre « security » et « safety »***
- ***Illustrer le concept de « security for safety »***
- ***Donner des exemples concrets de système aéronautique qui aborde ces différents concepts : « security », « safety » et « security for safety »***

## Plan de la présentation

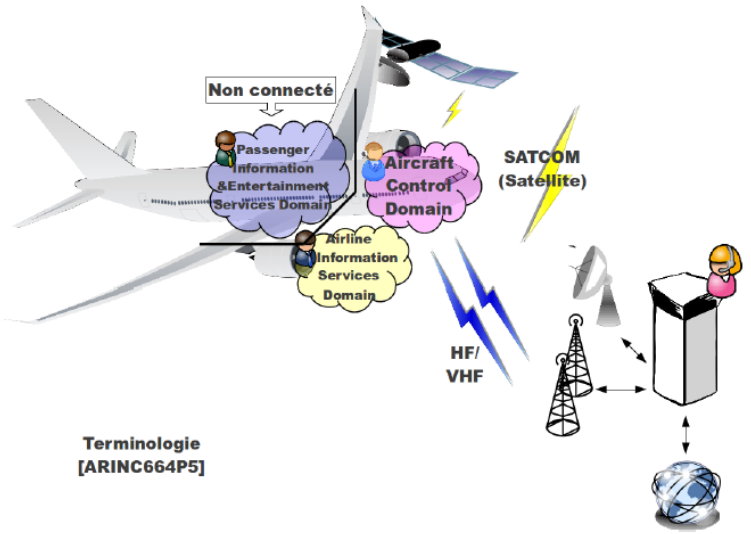
- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour traiter conjointement les aspects “security” et “safety”**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l’aéronautique**
- **Conclusion**



## Plan de la présentation

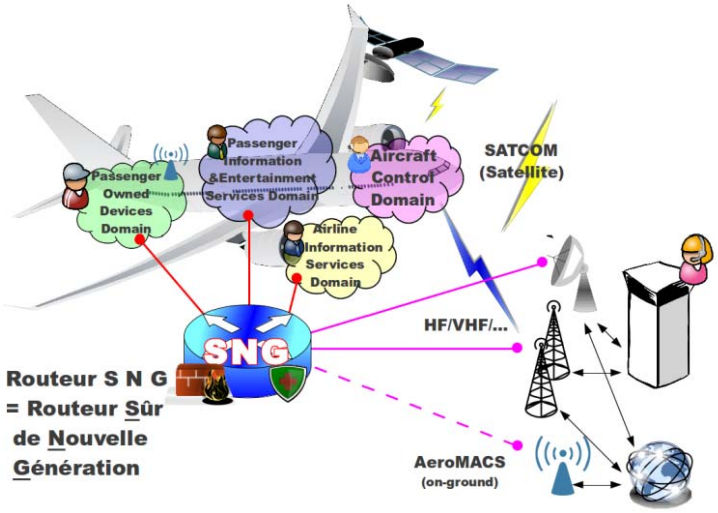
- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour traiter conjointement les aspects “security” et “safety”**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l’aéronautique**
- **Conclusion**

## Synthèse des domaines réseaux embarqués






## Interconnexion des réseaux avioniques



## Sûreté et sécurité : définitions

### Sécurité (transport)

La sécurité est la propriété d'innocuité du système, elle vise à protéger le système contre les défaillances et les pannes.
**Synonymes :** sûreté-de-fonctionnement, Sécurité-innocuité, «safety» en Anglais.

### Sûreté (transport)

La sûreté est la propriété d'immunité du système, elle qualifie la capacité d'un système à gérer les menaces et dangers externes au système.
**Synonymes :** sécurité informatique (hors domaine du transport) ! Sécurité-immunité, «security» en Anglais.

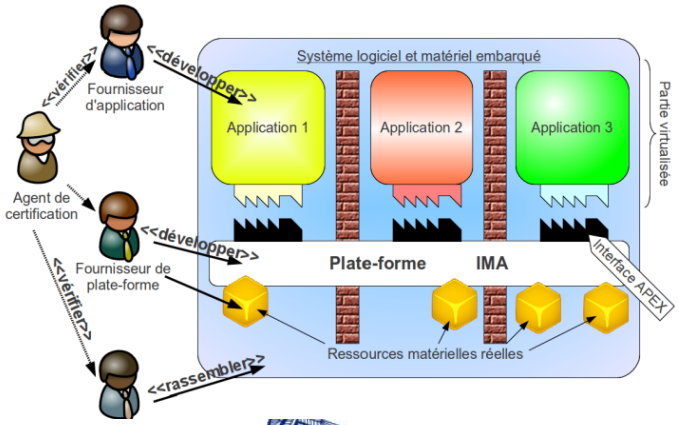
Sécurité et sûreté sont intimement liés
Pour classer, la question a se poser est : «*le risque est-il la conséquence d'un acte volontaire ou involontaire ?*»



## Architecture sécurisée : Integrated Modular Avionics

### Integrated Modular Avionics (IMA) [DO-297]

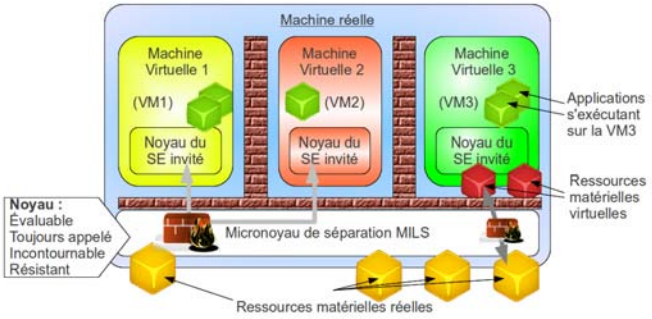
Norme définissant une **architecture** créée pour le **monde aéronautique**, en tenant compte des contraintes élevées de **sécurité**



## Architecture sûre : Multiple Independent Levels of Security

### Multiple Independent Levels of Security [Rushby 1981]

Créé pour le monde militaire, pour la **sûreté** des systèmes d'information, reposant sur un micronoyau de séparation exécutant des machines virtuelles (VM) isolées






## Vérification et validation de la sûreté et de la sécurité

### Sécurité : Certification

- [DO 178 B], [DO178C] : normes de certification du logiciel pour l'avionique
- Ecriture d'un **Software Requirement Specifications** (SRS) pour formaliser les besoins et fonctionnalités du routeur SNG et guider la certification du système

### Sûreté : Évaluation

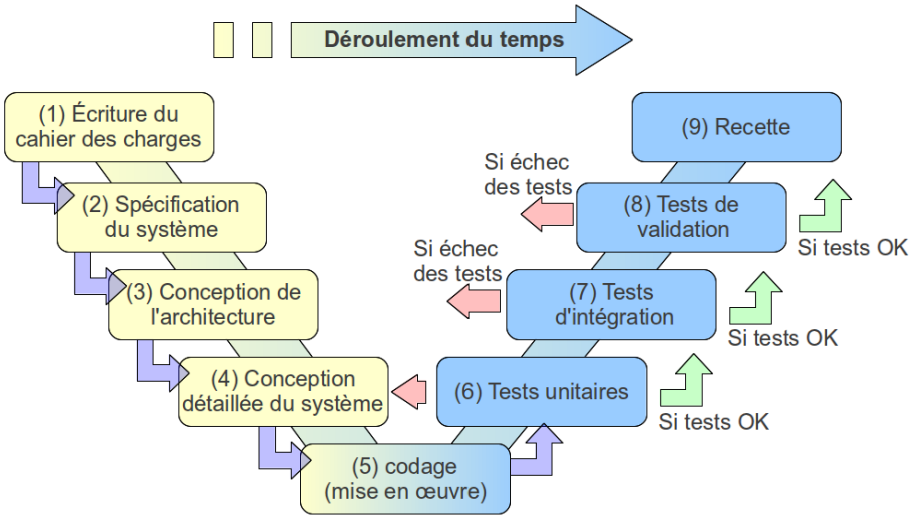
- [ISO 15 408] Critères Communs : norme utilisée pour évaluer la sûreté du routeur SNG
- Ecriture d'un **Profil de Protection** (PP) pour formaliser l'analyse et guider l'évaluation du Routeur SNG

## Outline

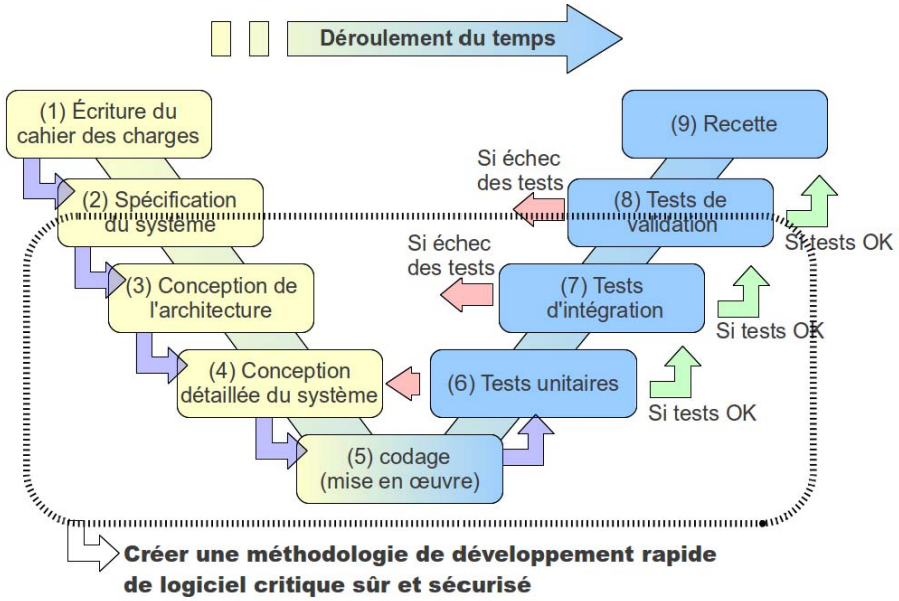
- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour traiter conjointement les aspects “security” et “safety”**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l’aéronautique**
- **Conclusion**



## Le cycle de développement en V



## Le cycle de développement en V



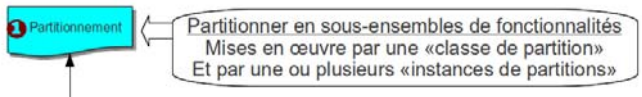



## Objectifs

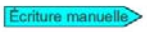
- Intégrer dans la réflexion initiale d'un produit les propriétés de « safety » et de « security »
- Ne pas voir les propriétés « security » comme disjointes des autres
- Ne pas attendre la fin du développement du produit pour vérifier si les propriétés de « security » sont vérifiées

## Une méthodologie générique en sept étapes

### Développement rapide de logiciel critique sûr et sécurisé



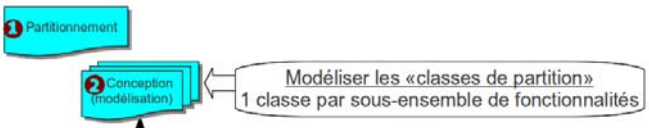

**Modularité :**
+ évaluation et certification facilitées
+ systèmes moins complexes que systèmes monolithiques
+ Parallélisation de la conception des classes de partition



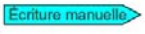



## Une méthodologie générique en sept étapes

### Développement rapide de logiciel critique sûr et sécurisé

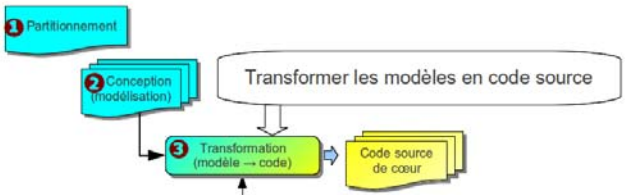



**Usage de modèles :**
+ Validation et correction au plus tôt (baisse des coûts)
+ Classes portables, réutilisables pour d'autres projets
+ Possible de créer des variantes dédiées au débogage
  ou au contrôle et de facilement intervertir entre les versions
+ Compatible avec la certification en suivant le [DO-331]
  (supplément du [DO-178C])

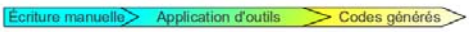


# Une méthodologie générique en sept étapes

## Développement rapide de logiciel critique sûr et sécurisé



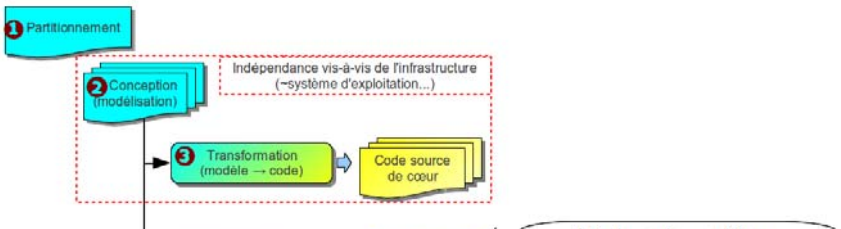

**Transformation automatisée** [Toom&al. 2010]
+ Rapidité de développement
+ Assurance que le code correspond parfaitement au modèle (pas d'erreur de conversion manuelle)
! Il faut valider l'outil de transformation



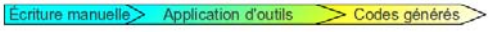



# Une méthodologie générique en sept étapes

## Développement rapide de logiciel critique sûr et sécurisé

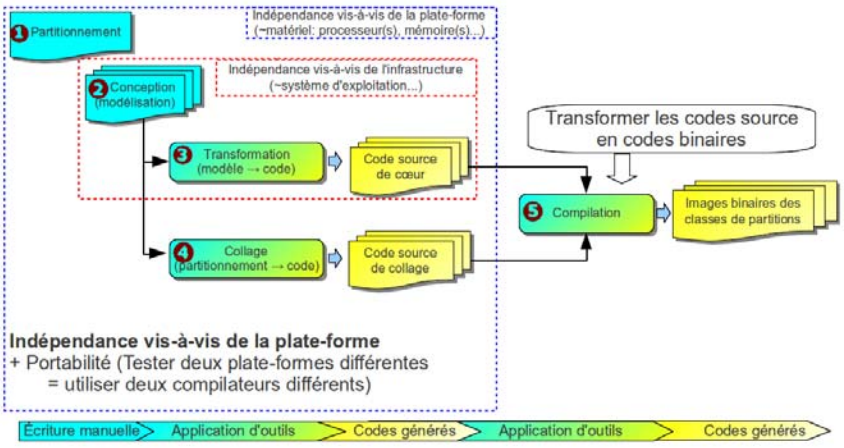



**Indépendance vis-à-vis de l'infrastructure**
+ Le concepteur est spécialiste de la partie métier, il n'a pas besoin de connaître avec précision le reste du système



# Une méthodologie générique en sept étapes

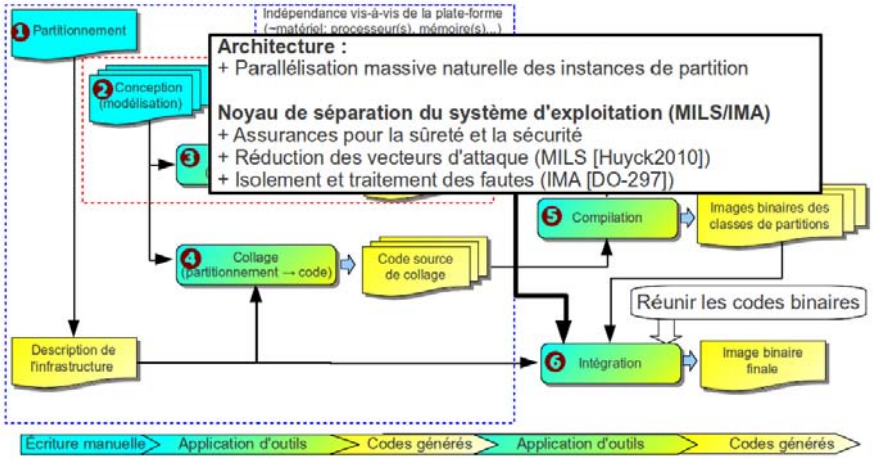
## Développement rapide de logiciel critique sûr et sécurisé





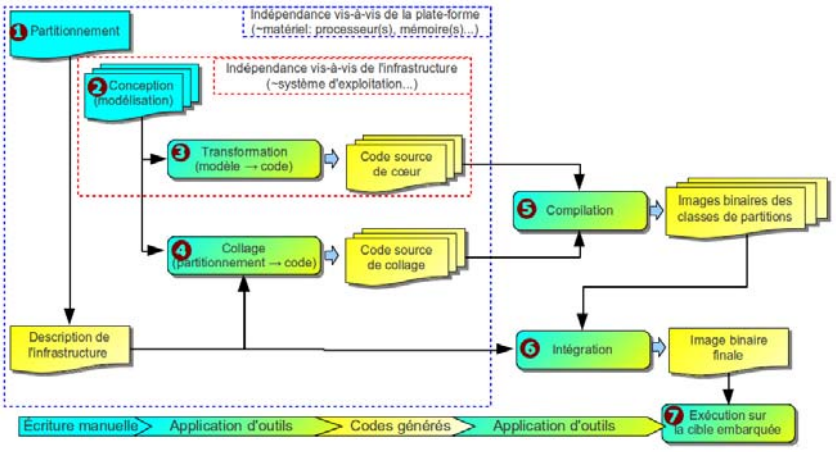

# Une méthodologie générique en sept étapes

## Développement rapide de logiciel critique sûr et sécurisé



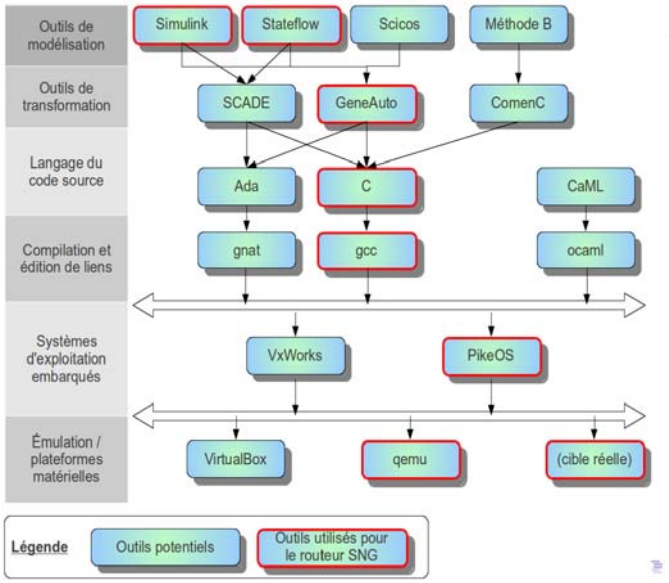
## Une méthodologie générique en sept étapes [DASC11]

### Développement rapide de logiciel critique sûr et sécurisé

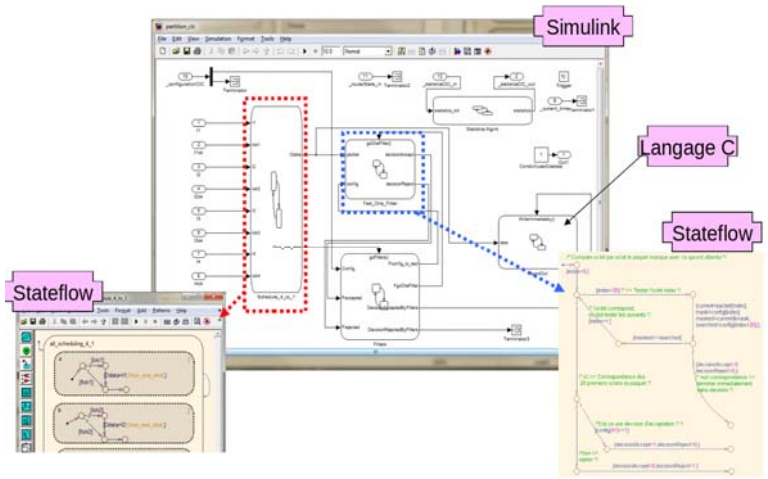





## Instanciation de la méthodologie



## Utilisation de cette méthodologie






## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation pour l'aéronautique**
  - **AeroMACS: vers du "Gatelink" sécurisé**
  - **Une PKI optimisée pour l'aéronautique**
  - **Le cas de la communication des drones**

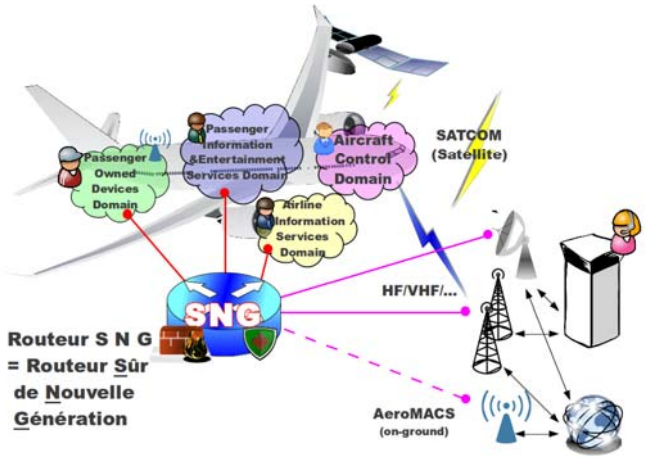
## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation pour l'aéronautique**
  - **AeroMACS: vers du "Gatelink" sécurisé**
  - **Une PKI optimisée pour l'aéronautique**
  - **Le cas de la communication des drones**



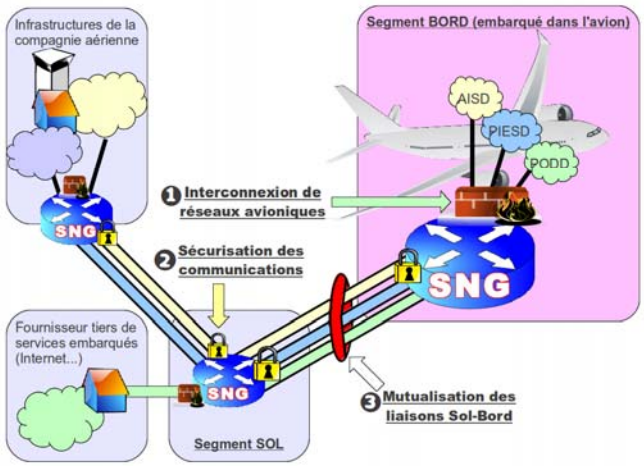
## Intérêt d'un routeur embarqué Sûr de Nouvelle Génération

Interconnexion des réseaux avioniques



## Intérêt d'un routeur embarqué Sûr de Nouvelle Génération

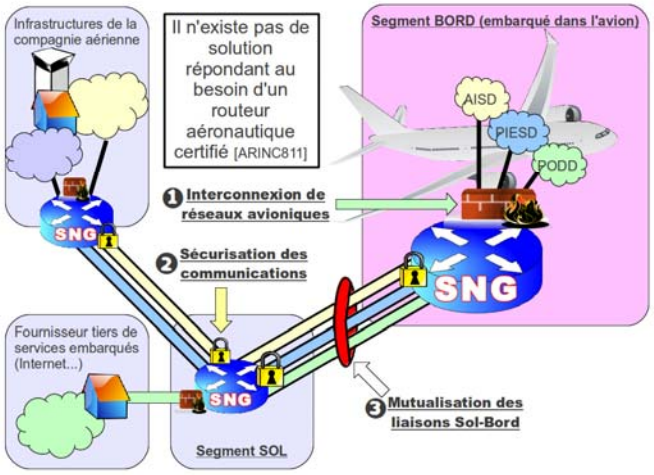
### Sécurisation et mutualisation des liaisons sol/bord






## Intérêt d'un routeur embarqué Sûr de Nouvelle Génération

### Sécurisation et mutualisation des liaisons sol/bord



## Projet SNG (Secure NextGen Router)

- Thèse CIFRE (2010-2013)
- Partenariat avec Thalès
- Définition des besoins du routeur SNG
- “Proof of concept” au travers d’une maquette à base de PC x86



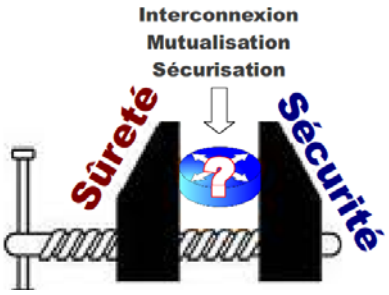
## Amélioration des communications de données pour un réseau de communication contraint

- Contexte *aéronautique* : **traitement conjoint** des approches “**security**” et “**safety**”
  - “Safety” : propriétés intrinsèques des systèmes leur permettant de résister aux **dysfonctionnements** (concept de sécurité-innocuité)
  - “Security” : protections contre les **menaces volontaires** (concept de sécurité-immunité)
- Pour une prise en compte :
  - Des niveaux d’**assurance logicielle** (DAL ou Design Assurance Level) “safety” permettant la **certification** du produit final (cf. [DO 178 B] et [DO 178 C])
  - **ET** des niveaux **d’évaluation** (EAL ou Evaluation Assurance Level) “security” permettant **l’évaluation** du système final (cf. [ISO 15 408])

## Vérification et validation de la sûreté et de la sécurité

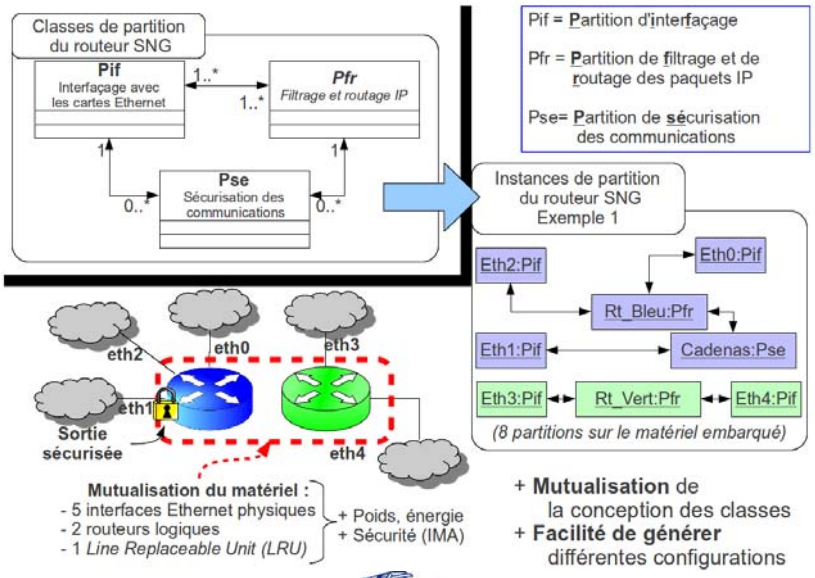
### Développement du routeur SNG : sûreté ET sécurité

Très contraignant, ce qui nous a conduit à élaborer une méthodologie de développement rapide de logiciel qui tienne compte de l'évaluation et de la certification du logiciel produit.

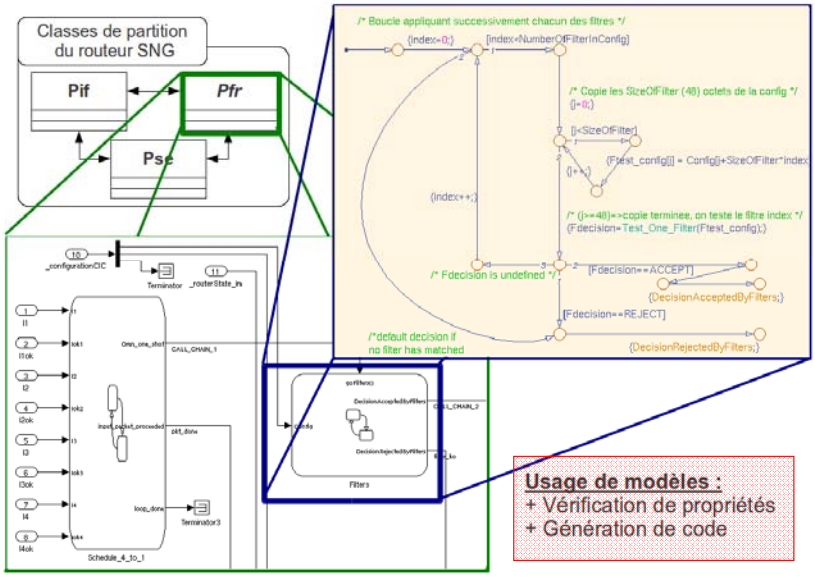





## Architecture du routeur SNG [ICNS11]



## Conception détaillée avec des modèles à états-transitions




**Usage de modèles :**
+ Vérification de propriétés
+ Génération de code



## Fonctionnalités de «security» du routeur SNG (Pse)

Trois services ciblés pour les communications de données aéronautiques

- Besoin de confidentialité
  - par ex: données techniques pour la compagnie, mails des passagers...
- Besoin d'intégrité
  - par ex: chargement des mises à jour des logiciels embarqués
- Besoin d'authentification
  - par ex: Controller Pilot DataLink Communications (CPDLC)

## Mise en œuvre de la sécurisation: protocole ESP

### Principe de fonctionnement

Les paquets IPv6 sont encapsulés dans d'autres paquets créés pour l'occasion, à l'aide du protocole *Encapsulating Security Payload* (ESP [rfc4303]).

### Spécificité du routeur SNG

La méthodologie permet la complémentarité entre du **code de "haut" niveau** (les modèles) et du **code de "bas" niveau** (codes sources des algorithmes AES-256, SHA-1, HMAC) :

- Performance du code bas niveau
- Vérifiabilité du code haut niveau



## Mise en œuvre de la sécurisation: protocole IKEv2

### Principe de fonctionnement

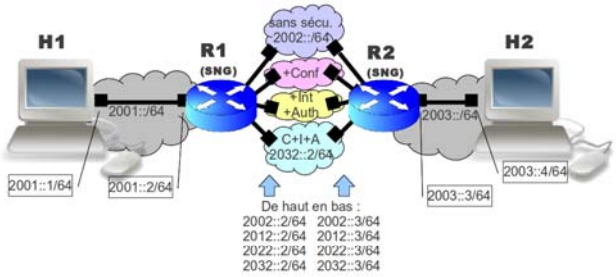
Le protocole *Internet Key Exchange version 2* (IKEv2 [rfc5996]) établit un chemin sécurisé appelé "canal" ou "tunnel" et négocie un jeu de clefs cryptographiques pour le protocole ESP.

### Spécificité du routeur SNG

Première mise en œuvre et validation de ce protocole de sécurité à l'aide de modèles :

- Vérifiabilité
  - Preuve formelle de terminaison
- Conformité du code binaire au modèle
  - Garantie par l'usage d'un générateur automatique de code

## Topologie de tests en environnement réel




Permet de valider les classes de partition :

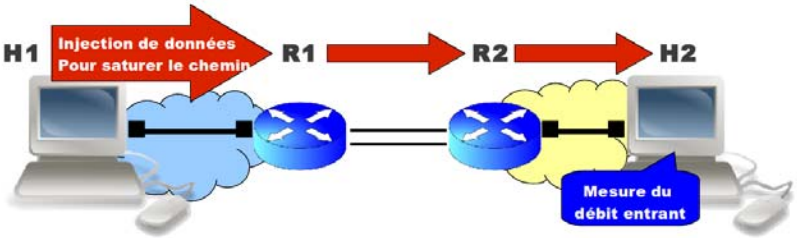
- [Pfr] le filtrage et le routage
  - pour l'interconnexion des réseaux,
- [Pse] la sécurisation des données
  - sécurisation et mutualisation des liens,
- [Pif] la connectivité

**R1 et R2**

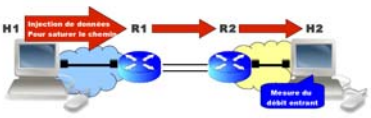
- Intel Xeon @1.6GHz
- RAM:2Go@800MHz
- Carte PCIe Ethernet 4-ports



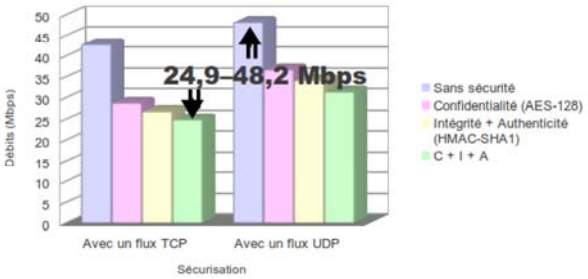
## 1/ Mesures de la capacité maximale du routeur SNG



## 1/ Mesures de la capacité maximale du routeur SNG




Impact des mécanismes de sécurisation sur le débit




- Chemin A/R symétrique,
- Full-Duplex,
- Matériels identiques
- Configurations symétriques

=> Débit maximal du chemin = capacité maximale de traitement offerte par le routeur SNG.



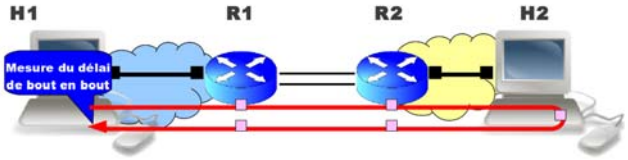
## Modélisation de trafic de charge multiflux aéronautique

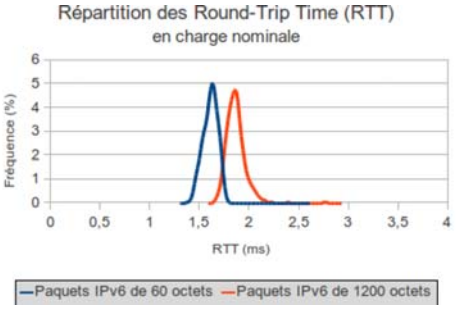
- Différents réseaux aéronautiques, différents besoins
- Trafic = ensemble de flux agrégés

| Flux | Débits | Type de flux et profil |
|---|---|---|
| critiques | 32.5 kbps | UDP, loi Uniforme *[cnes2009]* |
| non critiques (flux pas-sagers"APC") | • ~500 kbps descendant<br>• ~300 kbps montant<br>*[thales]* | 90% TCP et 10% UDP, Utilisation de sources ON/OFF Durées des flux: loi de Pareto Durées inter-flux: loi de Weibull *[gogoinf2013, orange2001, S.Gebert2012]* |

Caractérisation d'un profil ON/OFF réaliste pour l'*Aeronautical Passenger Communications* (APC)

## 2/ Mesures de délais, en fonction de la taille de paquets




$Délai_{maximal} = \frac{RTT}{4} \leq$ 500 µs



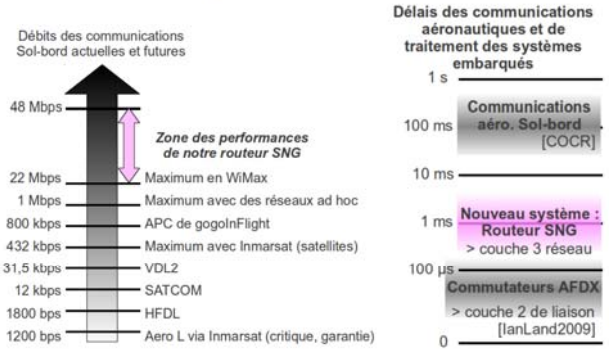
## Modélisation de trafic de charge multiflux aéronautique

- Création d'un logiciel ad hoc de génération de flux suivant le principe des sources ON/OFF : **sourcesonoff**,
  - http://www.recherche.enac.fr/~avaret/sourcesonoff, GPLv3, Open source, gratuit

**Bilan des expérimentations**

- L'impact du trafic de charge aéronautique est négligeable sur le comportement du routeur SNG, il est en effet bien inférieur aux capacités maximales de traitement du routeur.
- Débits supérieurs envisagés à long terme ($\geq$2020)

## Performances des systèmes aéronautiques actuels




Le routeur SNG, première mise en œuvre pour ce type de système aéronautique critique, valide les besoins identifiés en débits, délais et fonctionnalités.

Taux de 2.67E-6 paquets perdus sur 7 jours
(intégrité et disponibilité>99,999%).



## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation pour l'aéronautique**
  - **AeroMACS: vers du "Gatelink" sécurisé**
  - **Une PKI optimisée pour l'aéronautique**
  - **Le cas de la communication des drones**

## Pourquoi un protocole ?

### Quelques raisons

- Le besoin de sécurité des réseaux est de plus en plus présent
- La lourdeur de la configuration est un frein
- La sécurité niveau 3 (couche réseau):
  - généralement statique, peu de solutions dynamiques
- SCOUT permet la sécurité par le(s) routeur(s) d'extrémité(s) à la volée
  - et non plus seulement par les hôtes



## Ce que SCOUT ne fait pas


- Le protocole SCOUT
  - ne fait pas l'établissement du canal sécurisé
  - ne sécurise pas les données utilisateur
- SCOUT appelle et configure pour cela un protocole adéquat

## Ce que SCOUT fait

SCOUT essaye d'établir des canaux sécurisés pour les données, en fonction des capacités de sécurisation des noeuds du réseau qu'il découvre



## Taxonomie utilisée

**Inspirateur**

Le nœud qui transmet des données

**Initiateur**

Le nœud qui encapsule les données pour les sécuriser

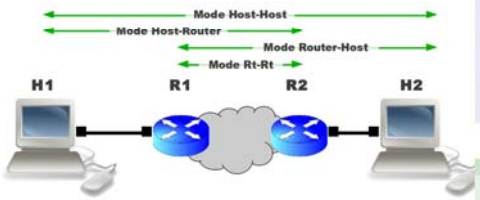
**Répondeur**

Le nœud qui décapsule les données sécurisées

**Destinataire**

Le nœud qui reçoit les données

## Les 4 modes de fonctionnement de SCOUT



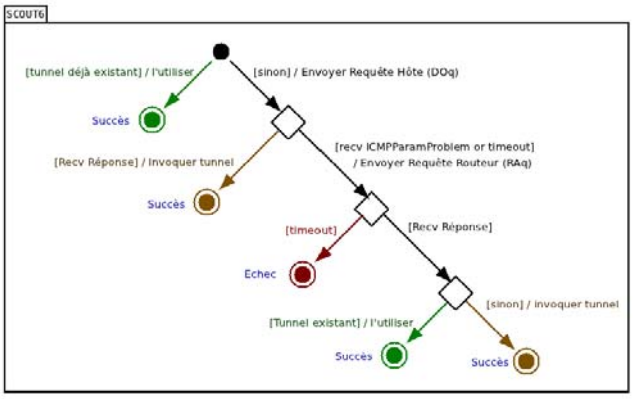

La sécurité dépend de la prise en charge de SCOUT sur les nœuds

| SCOUT mode | H1-R1 | R1-R2 | R2-H2 |
|---|---|---|---|
| Host-Host | ✓ | ✓ | ✓ |
| Host-Router | ✓ | ✓ | ✗ |
| Router-Host | ✗ | ✓ | ✓ |
| Router-Router | ✗ | ✓ | ✗ |

+ La section R1-R2 est sécurisée dans les 4 modes



## Algorithme de SCOUT



## Mise en œuvre avec IPv6 : le protocole SCOUT6

**Le protocole SCOUT**

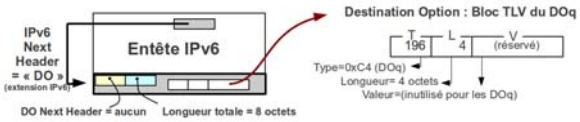
Protocole générique spécifiant les échanges et le principe général de fonctionnement de la découverte

**Le protocole SCOUT6**

Instanciation de SCOUT avec les fonctionnalités introduites par le protocole IPv6

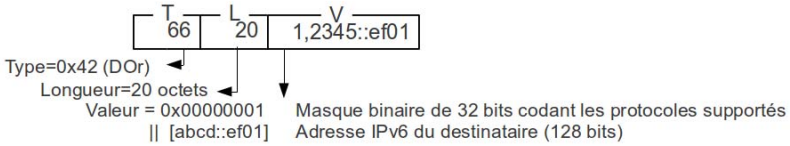


## La requête initiale "DOq"




- N°DOq 196: non assigné par l'IANA
  - "Destination Option query"
  - Emise par l'**initiateur**
  - Comportement par défaut du nœud: retourner un message ICMP Parameter Problem

## La réponse "DOr"




- N°DOr 66: non assigné par l'IANA
  - "Destination Option response"
  - Comportement par défaut du nœud: ignorer
  - Emise par le **répondeur**
- Masque binaire des protocoles supportés:
  - [(experimental) 0 ... 0 (KINK) (IKEv2) (IKEv1) ]/32



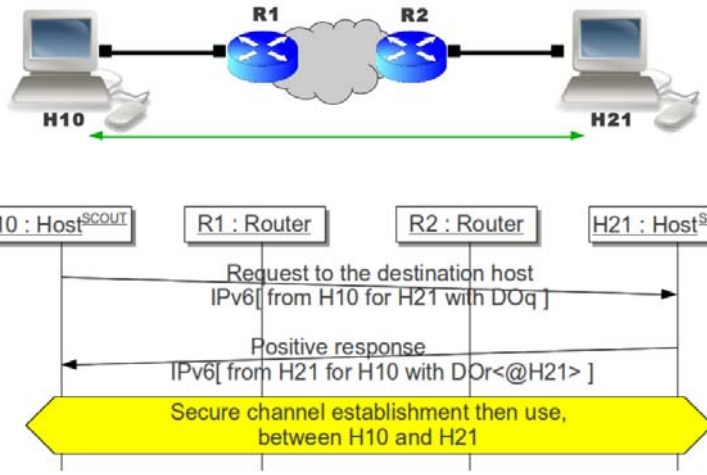
## La requête routeur "RAq"

- N°RAq 42: non assigné par l'IANA
  - "Router Alert query"

    *les routeurs faisant suivre le paquet traitent l'option si elles savent le traiter, l'ignorent sinon*

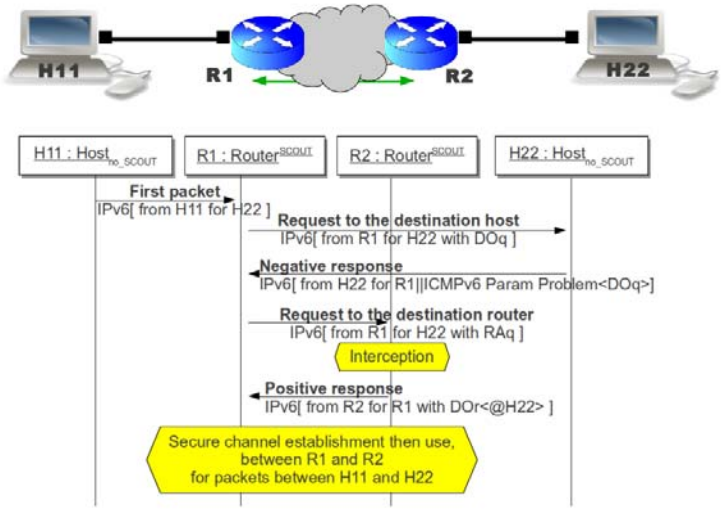
  - Idée= le routeur final s'assigne le rôle de répondeur

## SCOUT6 en mode Host-host

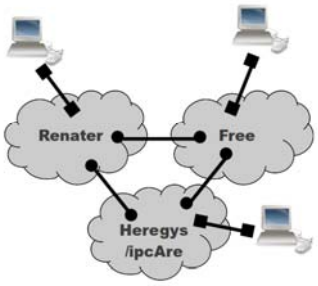





## SCOUT6 en mode Routeur-Routeur



## Validation sur Internet de SCOUT6

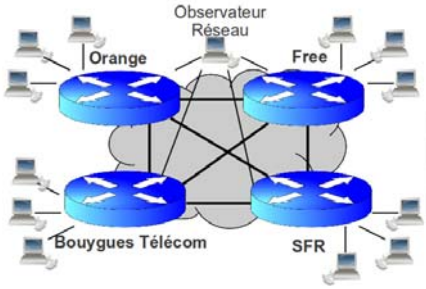



### Résultats en env. réel

- Les "Destination Option" sont toujours transmis
- Les "Router Alert" passent tous les peering, sauf de Free vers Heregys
- iptables considère les paquets "INVALID" car pas de user-payload
  - (ajouter des règles hbh et do)



## Contexte à 4 Fournisseurs d'Accès Internet émulés

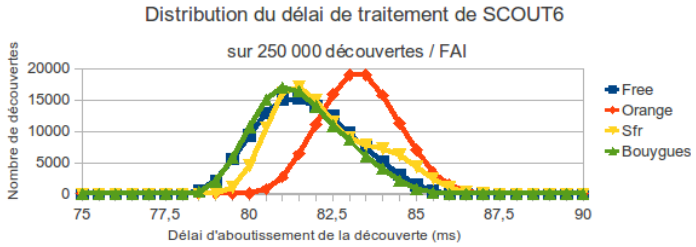



**Délais moyens et gigue (en ms)**

| | Orange | Free | SFR |
|---|---|---|---|
| BouygT | 41,1 / 1,7 | 37,6 / 0,5 | 39 / 0,4 |
| Orange | | 41,3 /1,6 | 42,7 / 1,8 |
| Free | | | 39,2 / 0,6 |

- 4 VM (VirtualBox): RAM 256 Mo, CPU 1.6GHz, Debian Squezze avec Traffic Control/netem
- Mesures des délais effectuées le 6 décembre 2011 à 11h00

## Mesure des délais d'acheminement de bout en bout




- Rapidité de la découverte
  - délai de traitement SCOUT << délai de transport
- Auto-configuration (pas de tunnel statiquement préconfiguré)
  - Mais authentification à prévoir + config en tant que "répondeur" à l'installation de SCOUT6



## Scout en « une diapo »

- Le protocole SCOUT détecte automatiquement les possibilités de sécurisation
- L'absence de sécurisation sur le noeud final peut être compensé par une sécurisation avec le routeur final
- Idem pour le noeud initial
- La configuration est plus légère qu'avec des tunnels statiques
- La surcharge réseau et le délai ajouté sont faibles

Implémentation téléchargeable sur...

http://www.recherche.enac.fr/leopart/~avaret/scout6/ :

- scout6_beta_2012-08-31.tar.bz2 (code source)
- package_debian/*.deb (src + binaire amd64 + binaire i386)

## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation pour l'aéronautique**
  - **AeroMACS: vers du "Gatelink" sécurisé**
  - **Une PKI optimisée pour l'aéronautique**
  - **Le cas de la communication des drones**



## Current ATM Communication Means

**Primary Mode: Voice**
DSB-AM (25 and 8.33 KHz)

**Limited Data Link:**
ACARS and VDL2

# SESAR project

- SESAR: Single European Sky for ATM Research
  - Future aeronautical communicaitons: > 2020
- WP 15.2.4 & 15.2.7: air ground communication architecture definition
  - AeroMACS is part of this architecture



## Future Communications

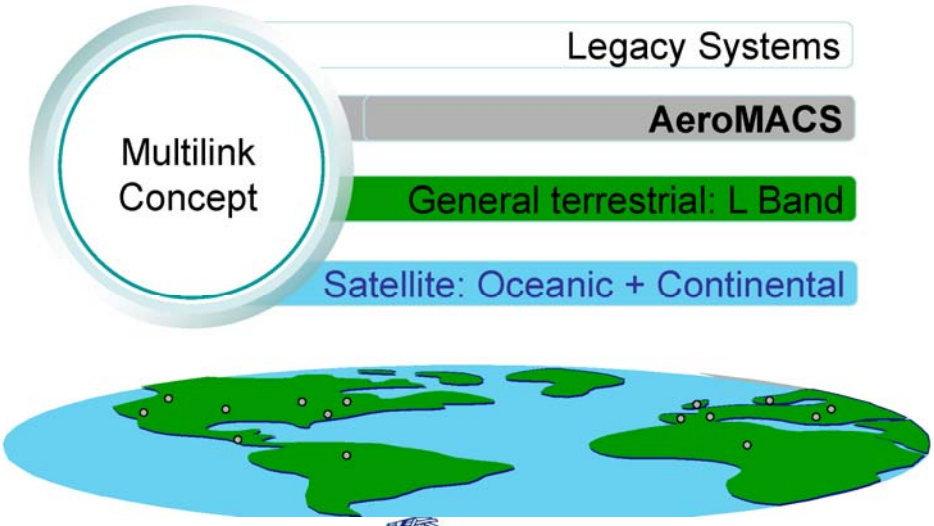
Future ATM concept requires **new ATM services**

**Data will be the primary mode** of future operations (voice mainly for emergency)

**No single technology** supports all requirements across all flight domains

Future Communications Infrastructure (FCI) will be a **system of systems** integrating existing systems as well as new systems

## Future COM Infrastructure






## Aeronautical Mobile Airport Communications System (AeroMACS)

- Mobile and fixed broadband wireless networked communications for the highest concentration of users in the National Airspace System: Airports
  - Air traffic control, airline operations, airport operations, safety services, situational awareness

## AeroMACS Applications

- Operation in ITU regulated spectrum (AM(R)S allocation offering protection from interference)
- AeroMACS Eligible communications cover:
  - Safety of Life (Air Traffic Management - ATM)
  - Regularity of Flight (Airline Operational Communications - AOC)



## Potential AeroMACS Applications - ATM

- DLL
- FLTPLAN
- D-OTIS
- DCL
- FLIPCY
- D-SIG
- LOADSHT
- D-ALERT
- D-TAXI
- OOOI
- …

## Potential AeroMACS Applications - AOC

**EFB related**
- Aircraft Briefing Cards
- Airworthiness Statement
- Crew Briefings
- Company NOTAMs
- De-icing request
- Delay reporting
- e-Charts (update)
- e-Graphical Weather
- e-Signature, e-Reporting
- Electronic Flight Folder
- Electronic Airway bill
- Flight Deck Duty Time registration
- Flight Deck Recency registration
- Flight Journal Documentation
- Fuel Tickets
- Notice to Captain
- Landing Performance calculation
- Onboard Video
- Passenger Information List/Manifest

**FOQA/FDR/ACMS related:**
- Aircraft Telemetry Service
- Emergency Data Transfer
- FOQA Data Transfer
- …

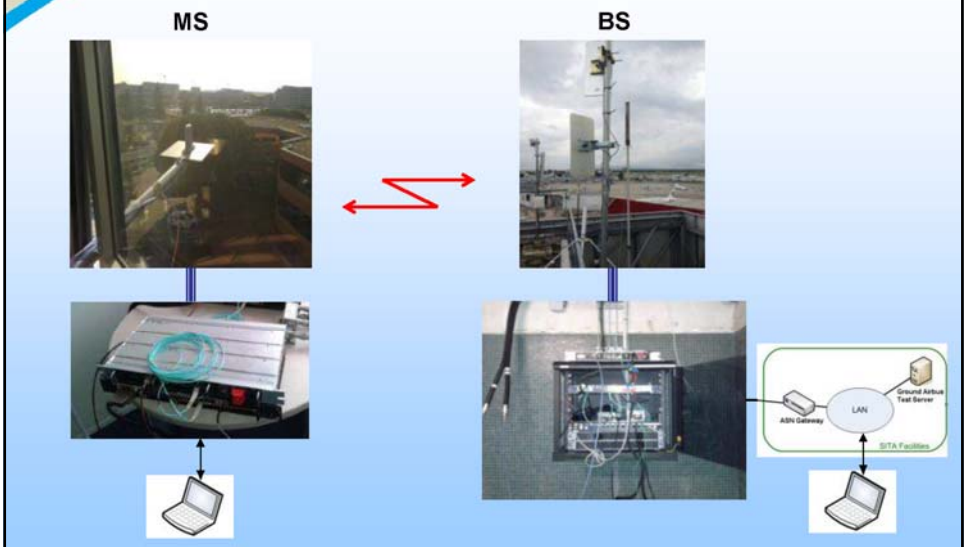
**Standard AOC Services:**
- Climb wind Uplink
- Descent Wind uplink
- ETOPS monitoring
- FMC Progress reporting
- ETA / ETA Management
- Hijack report
- Turbulence reporting
- ……

**Services with direct influence on operation:**
- Passenger Medical Examination
- Hijack Report



SANDRA

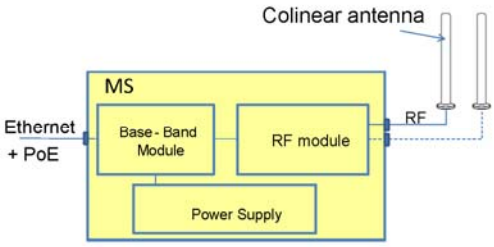
## Toulouse Airport
*AeroMACS MS/BS Installations*



## THALES AeroMACS MS prototypes

### Thales MS

- **Small form factor mobile station for vehicle integration**
  - all-in-one packaging of base-band and RF components
  - External collinear antenna (6 dBi)




Dimensions: ~ 300 x 300 x 90 mm
Weight : < 3 kg





## Airport Surface Research &Demos

Aeronautical Research Vehicle (ARV)

Sensor Systems MLS
5 GHZ Antenna

Sensis Mode S Vehicle
Locator 24-bit ICAO address

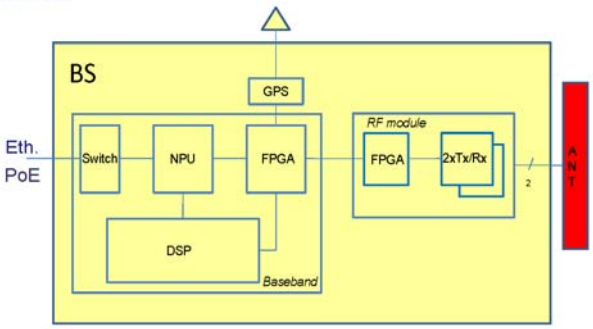
Viking S3-B

- FY10 Research
  - Network performance, mobile sector handoffs, blockage/ outage recovery, signal propagation
  - QoS data prioritization, data throughput, channelization
  - Security with authentication and encryption
  - Globalstar interference modeling
- FY10 Demos
  - Communication of MLAT surveillance data via AeroMACS
  - Emulate loading graphical weather products into cockpit
  - Establish Mobile AeroMACS Initial Operational Capability

## THALES AeroMACS BS prototype

### Thales BS

- All outdoor, compact architecture easy to deploy at the airport
  - all-in-one packaging of base-band and RF components
  - Integrated dual slant (+/- 45 ) sector antenna (15 dBi)
  - GPS for synchronization


Dimensions: ~ 400 mm x 375 mm x 130 mm
Weight : ~ 12 Kg

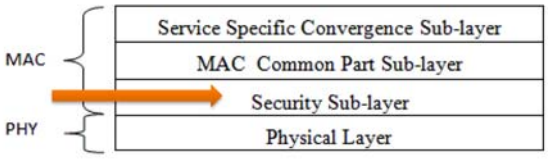


## AeroMACS Features

- **Quality of Service (QoS):**
  - throughput rate, packet error rate deleted, scheduling, time delay and jitter, resource management
- **Scalability:**
  - flexible bandwidth, channelization, enable growth on demand
- **Security:**
  - authentication, authorization, encryption, digital certificates
- **Privacy:**
  - support for private Virtual Local Area Networks (VLANs)
- **Commercial Leverage:**
  - Based on modern communications technologies and supports modern Internet-based network protocols
- **Lower Cost:**
  - Via commercial standards and components, WiMAX Forum™ industry capabilities, and reduced physical infrastructure

## The WiMAX Security Sub-layer

- AeroMACS **security is built on WIMAX security**
  - according to WIMAX forum specifications



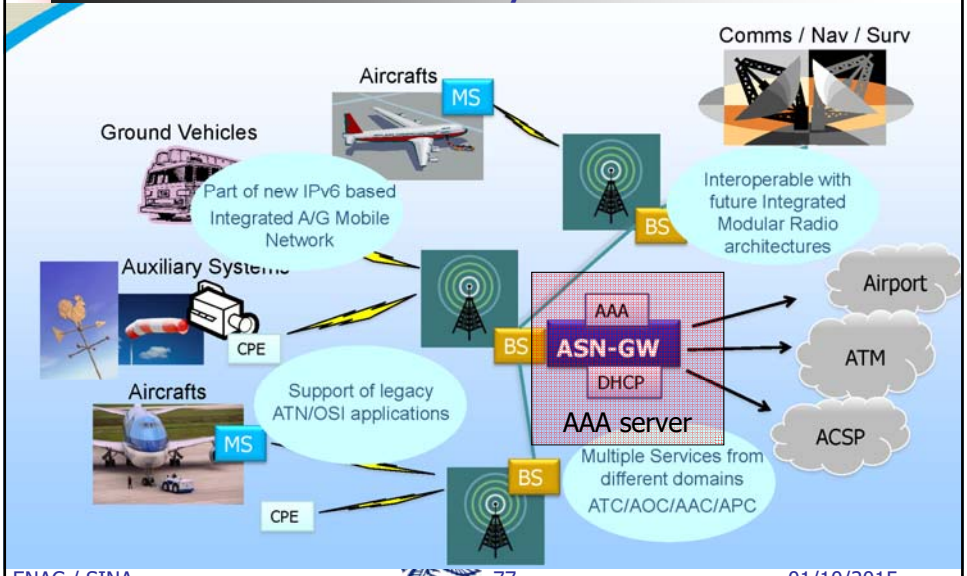



## The WiMAX Security Sub-layer

A High-Level Features List – the Architecture:

- Authorization Policy
- PKMv2 support
- EAP-based authorization
- CCM-mode with AES key-wrap
- Primary and static SA's
- Unicast SA (Multicast / Broadcast?)
- Encryption
- X.509

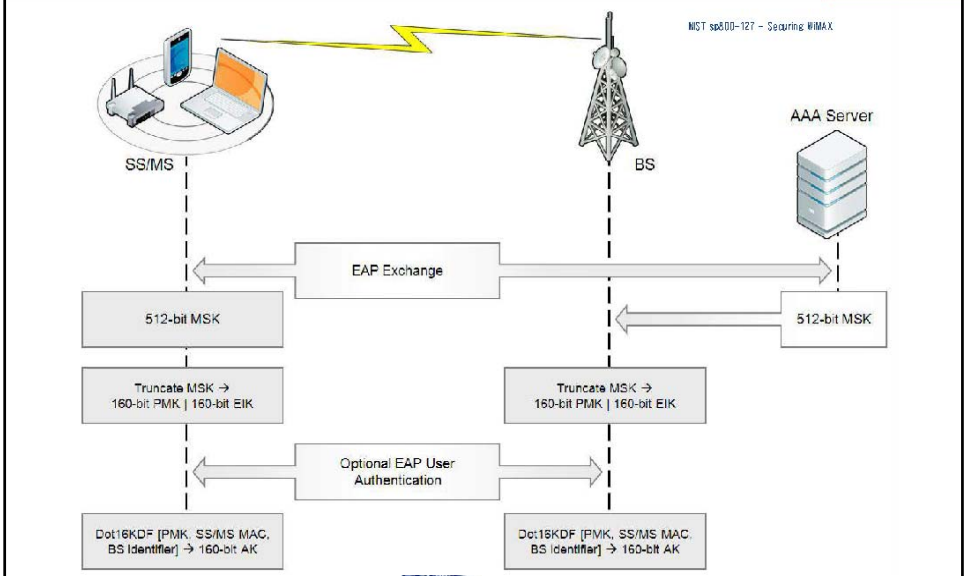
# AeroMACS security architecture






# EAP Authorization – Example of AAA Role

HITACHI
Inspire the Next



## Overview of Threats and Vulnerabilities

Jamming, Obstructions and Reflections

Unauthenticated and Unencrypted Messaging

- Unauthenticated SS may be allowed in the network
- Management messages are unencrypted (reveals MAC addresses and other attributes)

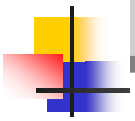
Base Station Masquerades – the Rogue BS

- MITM attacks may still be possible…

DOS Attacks

- Network entry requests by Rogue SS
- Corrupt packet insertions





## A Few Issues for Future Work

Certificates and Certificate Authorities

- Certificate chains, hierarchies…
- Which are the CA's?
- How many certificates in the chain?
- UN role? Jurisdictional role? Operator role? Manufacturer role? WiMAX Forum role?

- Need for **WiMAX security mechanism enhancements**
- Additional security mechanisms for AeroMACS: **work in progress** with EUROCAE, EASA and FAA, **finished in 2017**

## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation pour l'aéronautique**
  - **AeroMACS: vers du "Gatelink" sécurisé**
  - **Une PKI optimisée pour l'aéronautique**
  - **Le cas de la communication des drones**



## Public Key Infrastructure (PKI)

**What is it?**

Set of hardware, software, policies, people and processes

**Based on what?**

Asymmetric cryptography (Public / Private keys)

**For what?**

- Secure digital data (Confidentiality)
- Identity trust (Authentication of end entities)
- Unmodified data (Integrity)
- Distribute and manage keys and certificates (Scalability)

What value for future aircraft communications?

## PKI key role for future aircraft communications

### Security of aeronautical services

- Electronic distribution of airplane software (e.g. A380)
- Electronic Flight Bag
- Datalink purposes
  - ACARS Message Security (AMS)
  - CPDLC system
- Aircraft, crew, and devices identity management
- Broadband Internet service for passengers

### Scalability issues

- Heterogenous embedded entities $\times$ Number of flights
  - Passengers
  - Network devices

  $\Rightarrow$ Huge amount of keys and certificates to manage!!



## PKI: Advantages VS. Drawbacks

### Advantages

- Security
- Scalability

### Drawbacks

- Additional signalling overhead
  - Keys (e.g. 256 Bytes)
  - Certificates (e.g. 1 KByte)
  - Heavy Certificate Revocation Lists (CRLs)...

$\Rightarrow$ PKI has to be deployed at lower network cost

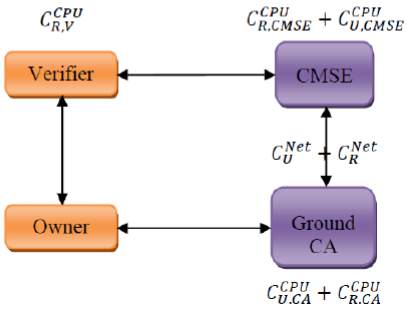
**Performance-aware hierarchical PKI model for future aircrafts communications**

## Standard PKI model: what's wrong with it?

**Network consumptions**

- Fixed ground CAs
- PKI credentials: air-ground link
- Excessive usage!!
  ⇒ Need to minimize overhead

**Hierarchical PKI model**





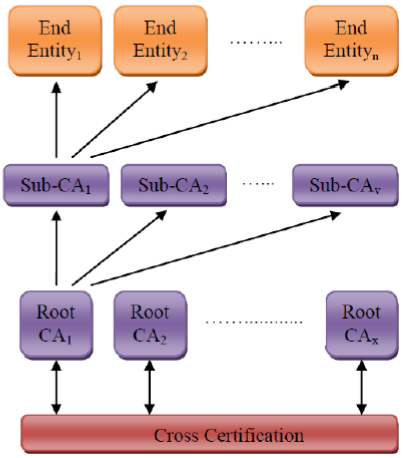

## Hierarchical PKI model: design principles

**Three levels**

1. Inter-CAs
   - Ground-located
   - Per airline
2. Root-CAs / Sub-CAs
   - Manage only sub-CAs

   ⇒ Minimize CAs workload
3. Sub-CAs / End entities
   - Manage end entities
   - ! Only passengers

⇒ Extend to other entities



## Considered approach

### 1 - Define PKI models

Standard PKI model VS Hierarchical PKI model

### 2 - Studied processes

1. Certificate generation and distribution
2. Certificate revocation

### 3 - Define three scenarios

- Certificate verifier and owner location (onboard or ground)
- Presented scenario: Ground verifier - Onboard owner

$\Rightarrow$ Analytic air-ground network costs for both models

### 4 - Extrapolate to real data statistics

Deduce results and compare both models



## Aircraft source data

### Use of real data statistics

- DSNA-DTI database
- Daily air traffic statistics in the French airspace
- Structured by hour of flight, ICAO code, and aircraft label

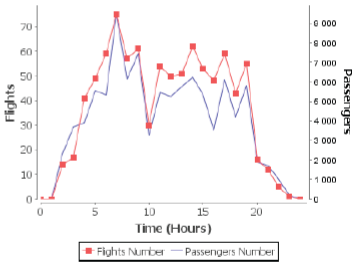
### Extract (useful) data

- Total number of aircrafts per hour
- Maximum number of carried passengers
  - Maximum seats capacity for each type of aicraft
  - Average aircraft filling between 70% and 80% (more realistic)
- Focus on one airline
  - Largest French airline (Air France)

## Aircraft source data: results

**Statistics**

- Average number of flights
  ⇒ 38 aircrafts per hour of flight
- Average number of passengers
  ⇒ 4,200 passengers per hour of flight




**What purpose?**

Extrapolate to scenarios



## Certificate generation and distribution process

**PKI model comparison**

Hierarchical PKI model VS. Standard PKI model

**Study parameters**

- RSA signature key length: 256 Bytes
- Certificate length: 1 KByte
- One certificate per user
- Exchanged data not considered
  ⇒ Only additional PKI signalling overhead is quantified here

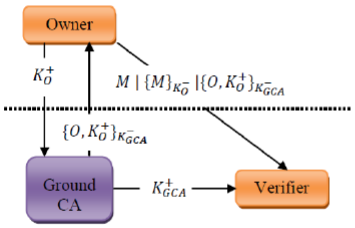
# Acronyms and notations

**Table 1. Notations**

| Notation | Description |
|---|---|
| $K_i^+$ | The public key of an entity $i$ |
| $K_i^-$ | The private key of an entity $i$ |
| $N_C$ | Total number of certificates |
| $N_f$ | Flight number at time $t$ |
| $Size_C$ | Average size of a certificate |
| $t_C$ | Certificate validity period (in days) |
| $t_S$ | SSP validity period (in days) |
| $h_S$ | Digest using a hash function |
| $Nonce_i$ | $i^{th}$ randomly generated number |
| $l_{sig}$ | Digital signature length |
| $l_{sn}$ | Certificate serial number length |
| $C_{sig}$ | Signature generation time |
| $C_v$ | Signature verification time |
| $M$ | Exchanged data |
| $\{i, K_i^+\}_{K_{CA}^-}$ | Certificate of $i$ issued by $CA$ |
| $R_C$ | % of revoked certificates |
| $N_R$ | Certificate revocation check status messages per day |
| $N_U$ | Revocation information update messages per day |
| $N_{C,CA}$ | Certificate average number handled by one $CA$ |
| $C_U^{Net}$ | Network cost to update a certificate between $CA$ and $CMSE$ |
| $C_{U,CA}^{CPU}$ | Computation cost at $CA$ to update a certificate |
| $C_{U,CMSE}^{CPU}$ | Computation cost at $CMSE$ to update a certificate |
| $C_R^{Net}$ | Network cost to check a certificate between $CMSE$ and a $verifier$ |
| $C_{R,CA}^{CPU}$ | Computation cost at $CA$ to check a certificate |
| $C_{R,CMSE}^{CPU}$ | Computation cost at $CMSE$ to check a certificate |
| $C_{R,V}^{CPU}$ | Computation cost at $verifier$ to check a certificate |

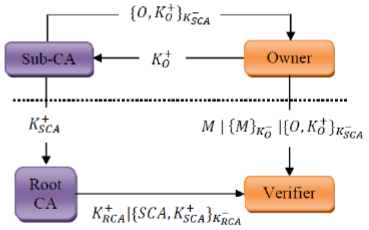


# Scenario 1: ground verifier / onboard owner




**Standard PKI model**

$2.N_C.(l_{sig} + Size_C)$




**Hierarchical PKI model**

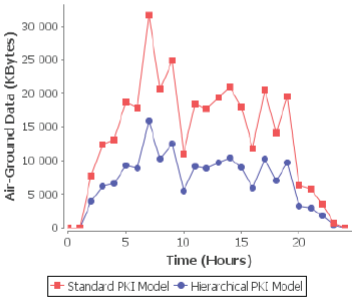
$N_f.l_{sig} + N_C.(l_{sig} + Size_C)$

## Scenario 1: results

**Performances**

- $Size_C \gg l_{sig}$
  $\Rightarrow$ More certificate exchanges in standard model
- $N_C \gg N_f$
  $\Rightarrow$ More air-ground exchanges in standard model

Measured average improvement: **55%**






## Results for scenarios 2 and 3

**Scenario 2**

- Onboard verifier - ground owner
- Secure web browsing (https)
- Measured average improvement: **20%**

**Scenario 3**

- Onboard verifier - Onboard owner
- Intra-domain AOC information exchange
- Measured average improvement: **92%**

## Certificate revocation process

### Considered revocation techniques

- RTCA specification 42 document guidlines
  - Certificate Revocation Lists (CRLs)
  - Online Certificate Status Protocol (OCSP)

### Simulation parameters

- Revocation update frequency: 24 hours
- RSA signature key length: 256 Bytes
- Certificate serial number lengh: 20 bits
- Signature time (RSA-based): 420 msec
- Vertification time (RSA-based): 0.113 msec
- % of revoked certificates: 10 %



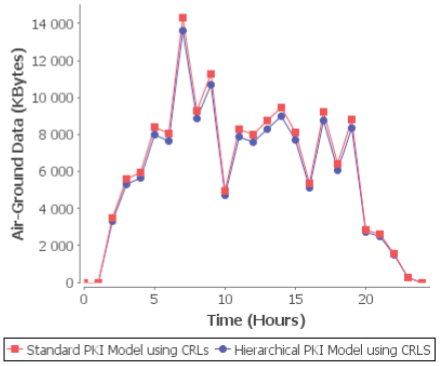
## Costs for updating certificate revocation information

### OCSP performances

- Network cost is null (co-located with CA)

### CRL performances

- Network costs: nearly the same for both models
- Computation cost $\simeq$ 48 msec for both models



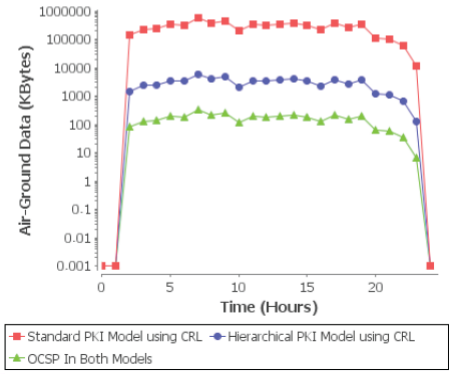
## Costs for revocation requests

**OCSP vs. CRLs**

- OCSP: Only one signature per revocation request
- CRLs: Too heavy compared to OCSP request messages

**OCSP is recommended for certificate revocation process**

Logarithmic scale!






## Summary

**Hierarchical PKI model for future ATM systems**

- Hierarchical CAs / Sub-CAs
- Simulation based on real traffic data

**Performance study**

- Certificate generation and distribution process
  - Hierarchical PKI model
  - Standard PKI model
- Revocation approaches
  - CRL
  - OCSP

## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation pour l'aéronautique**
  - **AeroMACS: vers du "Gatelink" sécurisé**
  - **Une PKI optimisée pour l'aéronautique**
  - **Le cas de la communication des drones**



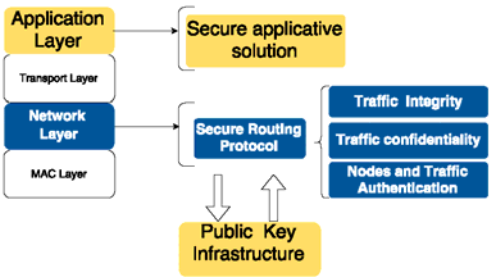
## SUANET: secure UAANET

Thèse CIFRE: 2014-2017

delair-tech AIRBORNE SENSORING

**SUANET research objectives**

**Objective** : Propose a secure and certified secure communication architecture for UAVs



## Plan

1. Introduction et contexte du travail
2. Élaboration d'une méthodologie de prototypage rapide
3. Création du protocole SUAP (Secure UAV Ad hoc routing Protocol)
4. Validation des performances du protocole SUAP
5. Conclusions & Perspectives

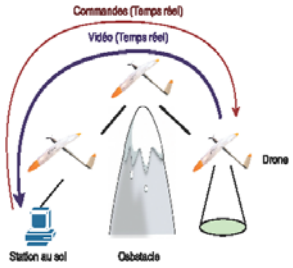




## Drones civils

- **Drones dans les missions civiles**
  - Plusieurs dimensions et nouvelles capacités
  - Plusieurs applications (ex : surveillance, cartographie, etc.)

## Drones civils



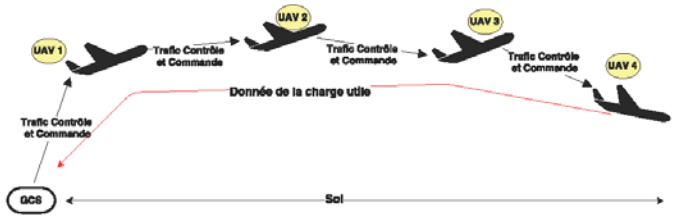

- **Drones dans les missions civiles**
  - Plusieurs dimensions et nouvelles capacités
  - Plusieurs applications (ex : surveillance, cartographie, etc.)
- **Flotte de drones coopératifs**
  - Variété de tâches
  - Niveau élevé de coordination (échange continu de données)
- **Différentes architectures de communication possible**
  - Architecture centralisée, réseaux satellites, réseaux cellulaires, réseaux ad hoc sans fil

Le réseau ad hoc sans fil est une solution prometteuse





## Pourquoi un réseau Ad hoc ?




### Réseau UAANET (UAV Ad hoc Network)

- Réseau ad hoc mobile (MANET - Mobile ad hoc Network) où les nœuds sont des drones
- Caractéristiques spécifiques :
  - Faible densité de nœuds, mobilité spécifique (3D), connectivité intermittente.

## Overview of UAANET

Nodes in UAANET are :

1. UAVs : to carry payload, on-board GPS and autopilot ;
2. GCS : to provide interface of the scanned zone and to transmit control traffic.

Delair Tech UAV Copyright

Delair Tech GCS Copyright





## Besoins de sécurité

### Vulnérabilités des réseaux MANET

- Canal de communication vulnérable
- Absence d'une ligne de défense
- Problème de coopération
- Existence des attaques

### Attaques sur le routage

- Attaque Blackhole : génération des faux paquets pour proposer de meilleures routes
- Attaque Wormhole : coordination entre deux ou plusieurs attaquants pour créer un tunnel et intercepter le trafic

### Besoin en sécurité

- Le protocole de routage doit être fiable en présence d'attaquants
  1. L'authentification des paquets de routage est importante pour la survie de la mission
  2. Les attaques ne devraient pas falsifier le choix d'une route

## Contexte *UAS* :

**UAANET**: UAv (Unmanned Aerial Vehicle) Ad hoc NETwork

Spécificités (par rapport aux autres types de MANET)

- **Faibles ressources** énergétiques et CPU (par rapport VANET ou AANET)
- **Modèles de mobilité** différents (par rapport à des déplacements rectilignes de type VANET)
- Comportements **autonomes ou semi-autonomes** (liaisons bi-directionnelles air sol et / ou entre drones, non présentes en WSN)

Prises en compte pour la définition de **mécanismes de routage**, de garantie de la **QdS** ou encore de **sécurité du réseau**





## Contexte de travail : vérification et validation de la sûreté pour une flotte de drones

**Sûreté de fonctionnement**

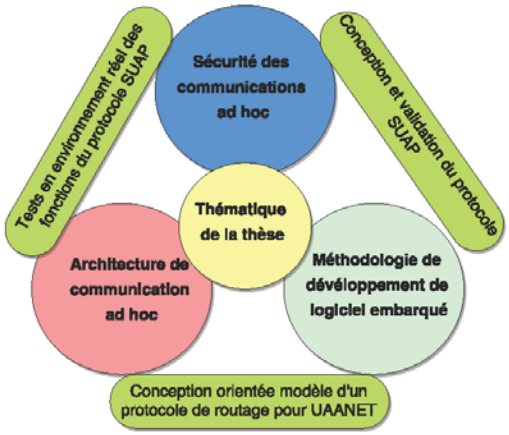
- Anticiper les défaillances et les pannes
- [DO 178 B], [DO 178 C] : normes de certification du logiciel pour l'avionique
- Vérification de conformité entre le code source et l'architecure logicielle durant la conception

**Besoin de validation**

- Assurer que la flotte de drones n'entre pas en collision avec d'autres systèmes (UTM : UAS Traffic Management)
- Nécessite une méthodologie qui prenne en compte l'évaluation et la certification du logiciel produit

Contribuer à la validation (dans le but d'obtenir une certification) du système UAS utilisé

## Domaines de recherche et contributions de la thèse

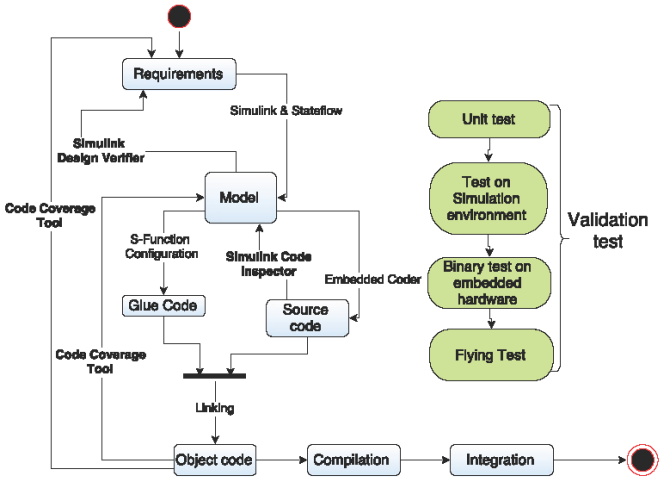







## Plan

## SUANET development process

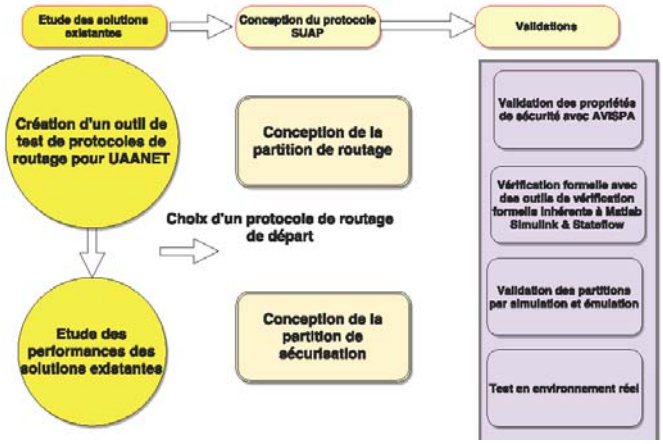







## Plan

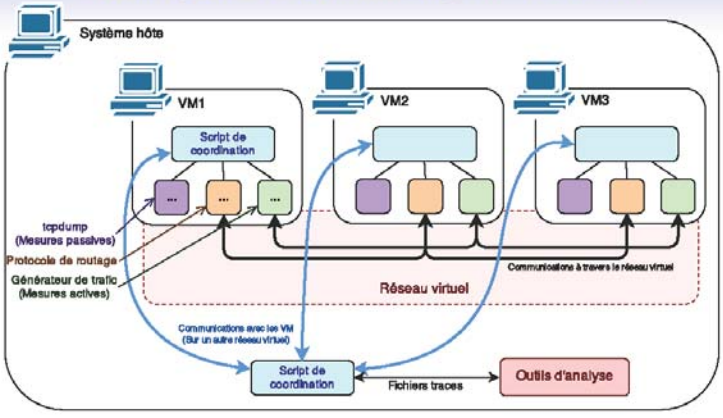
## Processus de conception et de validation du protocole SUAP








## Outil hybride d'évaluation pour UAANET



## Etude des protocoles de routage existant

### Cadre d'étude

1. Modélisation d'environnement UAANET sous OMNET++
   - Développement d'un module de mobilité rejouant des trajectoires réelles
   - Execution des protocoles dans un système d'exploitation émulé (machine virtuelle VirtualBox)
   - Implémentation en C des algorithmes de routage utilisés
   - Génération des trafics réels (trafic C2 et charge utile)
2. Comparaison des protocoles AODV, OLSR et DSR en environnement UAANET

AODV offre de meilleurs résultats en matière de taux de connectivité, délai de bout en bout, «overhead» et délai de reconstruction d'une route

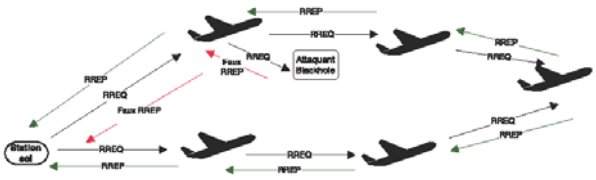




## Mise en œuvre de la sécurisation

### Motivation

- Partition de routage (basée sur AODV) reste vulnérable à différentes attaques
  - Par exemple, l'attaque blackhole



## Mise en œuvre de la sécurisation

### Motivation

1. Partition de routage (basée sur AODV) reste vulnérable à différentes attaques
   - Par exemple, l'attaque Blackhole
2. Services ciblés pour la sécurité du routage
   - Authentification des messages (pour les champs non mutables)
   - Intégrité des messages (pour les champs mutables)

### Mécanismes de sécurité des MANET existant

1. Plusieurs protocoles de routage de sécurité existant
   - ARAN, SAODV (Secure AODV), SEAR, SEAODV, ARIADNE, etc..
2. Choix de SAODV après une analyse de sécurité de l'existant
   - Authentification par signature des champs non mutables (par ex : adresse IP du nœud source)
   - Intégrité des champs mutables (par ex : nombre de sauts)

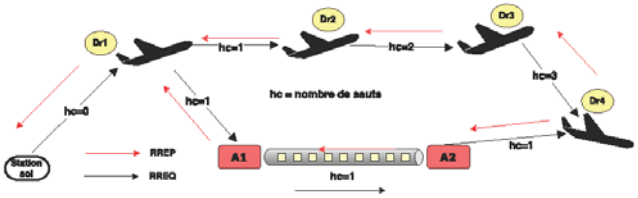




## Vulnérabilités du protocole SAODV

SAODV est vulnérable à des variantes de l'attaque wormhole

- Consiste à faire croire à deux nœuds distants qu'ils sont voisins
- Par exemple, création d'un tunnel wormhole



## Objectif du protocole SUAP

**Proposer une route fiable**

1. Authentifier les messages de routage
   - Eviter les modifications non autorisées des messages de routage
   - Eviter les attaques conduisant à la dégradation de performance
2. Protéger contre l'attaque wormhole
   - Assurer que les paquets de routage ne passent pas par un tunnel wormhole durant le processus de routage





## Modèles réseau et de sécurité considérés

- Nœuds homogènes
- Pas de restriction de ressources (énergie, mémoire, bande passante)
- Les drones utilisés sont munis d'antenne omnidirectionnelle
- Les nœuds sont synchronisés (les drones sont équipés de GPS)
- Nous supposons l'existence d'un système de gestion des clés pour partager les clés utilisées

## Mécanismes proposés

### Raisonnement

- L'attaque wormhole diminue d'une manière significative le nombre de sauts d'une source vers une destination.
- Il est possible de connaitre la distance relative entre deux voisins (synchronisation des nœuds)
- On considère le problème en deux dimensions

### Proposition

- Relation entre le nombre de sauts et la distance géographique entre les nœuds
- Inclusion de l'identité des nœuds légitimes dans le calcul de l'empreinte (valeur de hash)





## Mécanismes de sécurité contre l'attaque wormhole

**Les étapes de notre proposition**

**ETAPE 1 (à l'initialisation) :**
**Découverte de voisin**

**Rélation entre nombre de sauts et distance rélative**

**Authentification (des messages) entre voisin et vérification de l'existence d'un tunnel wormhole**

## Mécanismes de sécurité contre l'attaque wormhole

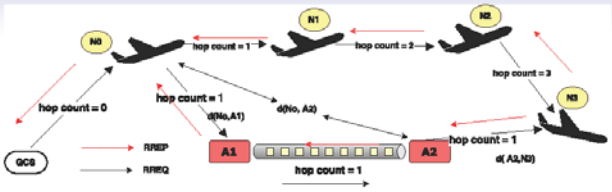
**Pour les paquets de découverte de voisin (paquet Hello)**

- Chaque nœud inclut sa position dans le paquet de découverte de voisin et le signe
- Calcul de la distance relative entre deux nœuds
- Le nœud récepteur vérifie la signature et calcule le nombre de sauts (virtuels) associés à la distance
- Comparaison des deux valeurs de nombre de sauts (à la réception) et déduction de l'existence d'un tunnel wormhole





## Illustration de l'échange des paquets Hello




T = distance totale de la route légitime
hc = valeur virtuelle du nombre de sauts

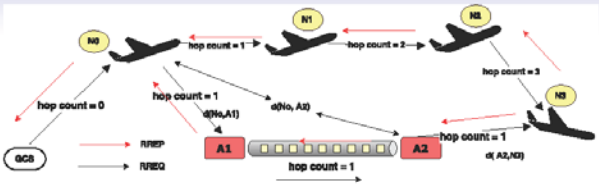
$$\frac{T}{Dmax} - 1 \leq hc < \frac{T}{Dmax} + 1 \quad (1)$$

avec

$$T = \sum_{i=0,j=0}^{n} R_{i,j}$$

- N0 envoi un paquet Hello au nœud N1
- N1 calcule la distance relative et déduit la valeur virtuelle du nombre de sauts
- N1 compare le nombre de sauts virtuel avec le nombre de sauts inclus dans le paquet.

## Illustration de l'échange des paquets Hello




T = distance totale de la route légitime
hc = valeur virtuelle du nombre de sauts

$$\frac{T}{Dmax} - 1 \leq hc < \frac{T}{Dmax} + 1 \qquad (1)$$

avec

$$T = \sum_{i=0,j=0}^{n} R_{i,j}$$

- N0 envoi un paquet Hello au nœud N3 à travers le tunnel
- N3 calcule la valeur virtuelle du nombre de sauts
- N3 compare les deux valeurs de nombre de sauts et constate l'anomalie





## Mécanismes de sécurité contre l'attaque wormhole

**Les étapes de notre proposition**

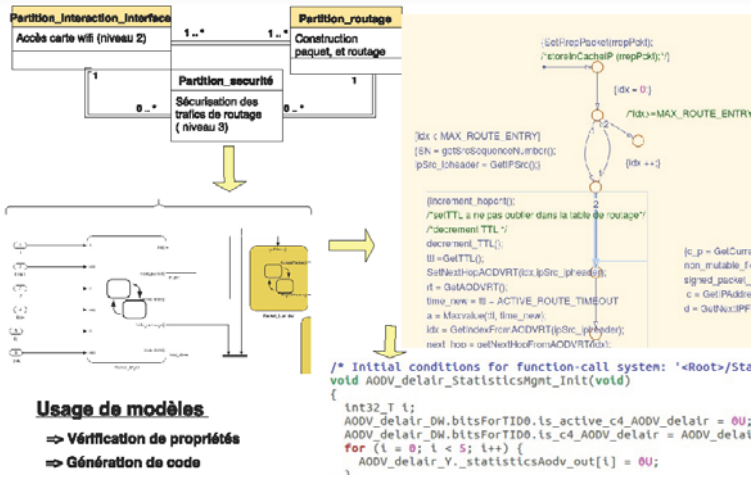
**ETAPE 1 (à l'initialisation) : Découverte de voisin**

- Rélation entre nombre de sauts et distance rélative
- Authentification (des messages) entre voisin et vérification de l'existence d'un tunnel wormhole

**ETAPE 2 : Découverte de route**

- Prise en compte de l'identité des noeuds dans le calcul de hash

## Mise en œuvre grâce à des modèles à états-transitions




**Usage de modèles**

=> Vérification de propriétés

=> Génération de code





## Plan

## Validation des classes de partition

**Test en environnement réel**

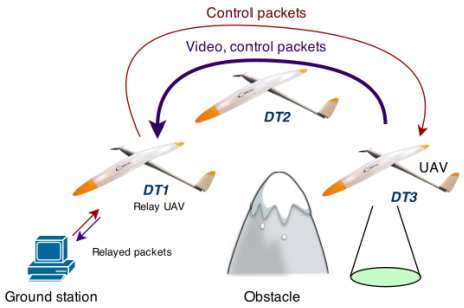
- Réalisé avec des drones DT 18 et des stations sol DT.
- Validation de la partition de routage
- Validation de la partition de sécurisation
  - Vérification de l'intégrité des messages (cas réel d'une attaque blackhole)
- Mécanismes de sécurité contre l'attaque wormhole non évalué en environnement réel

**Test en simulation et émulation**

- Utilisation de l'outil hybride de test
- Validation de la partition de routage
- Validation de la partition de sécurisation
  1. Vérification de l'intégrité des messages
  2. Vérification des mécanismes contre l'attaque wormhole
- Comparaison des performances de SUAP avec AODV



## SUANET application scenario




**Secure routing protocol requirements**

- UAV and Traffic authentication
- Data integrity
- Data confidentiality
- Preserve network resources for effective data exchanges

## Flying testbed




## Flying validation tests

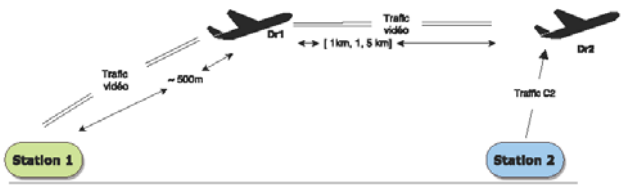
## Validation de la partition de routage

**Test en environnement réel**





## Topologie de test pour les fonctions de routage




Permet de valider la classe de partition de routage

- Routage du trafic temps réel
- Connectivité des différents nœuds

- Protocole AODV modélisé
- IEEE 802.11g

## Résultats de performance de SUAP par rapport à AODV

| Paramètres | Résultat d'émulation du protocole AODV | Test réel du protocole AODV modélisé |
|---|---|---|
| Taux de pertes | 3.05 % | 3.50 % |
| Délai moyen de bout en bout | 5.32 ms | 5.49 ms |
| Délai moyen de rétablissement de route | 1.94 ms | 2.08 ms |
| Durée de vie moyenne d'une route | 18.53 s | 14.34 s |
| «overhead» | 501 ko (0.034 %) | 552 ko (0.05 %) |

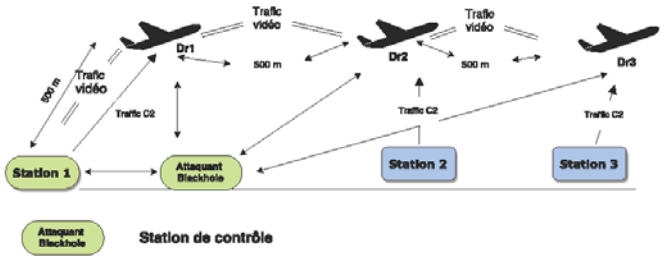




## Validation de la partition de sécurisation (authentification des messages)

Test en environnement réel

## Topologie de test pour les fonctions de sécurité




Permet de valider les classes de partition de sécurisation des trafics de routage

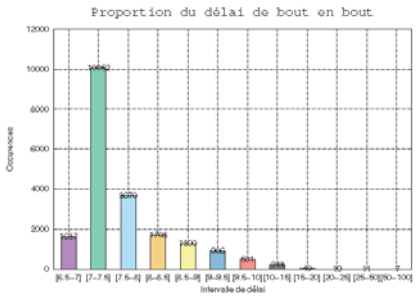
- Fonctions d'authentification et d'intégrité

- Protocole AODV modélisé et SUAP modélisé
- IEEE 802.11g





## Délai de bout en bout et délai d'acheminement des trafics vidéo

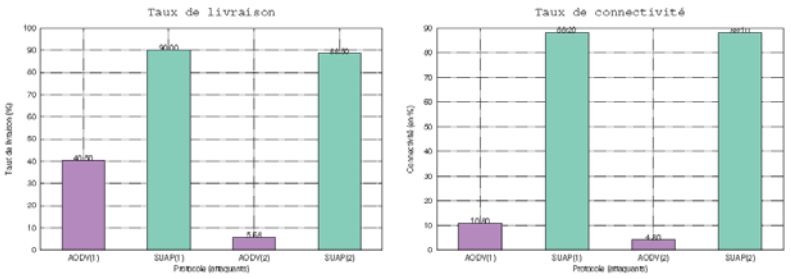



| Délai pour trafic de signalisation | Valeurs |
|---|---|
| Délai moyen | 7.43 ms |
| Délai maximum | 100 ms |
| **Délai pour trafic de charge utile** | **Valeurs** |
| Délai moyen | 9.2 ms |
| Délai maximum | 104 ms |

**Conclusion**

- Le délai nécessaire pour authentifier les paquets ne pénalise pas l'échange des trafics temps réel

## Taux de connectivité et de livraison des données




### Conclusion

- AODV souffre de l'effet de l'attaque blackhole.
- Avec SUAP, la connectivité est maintenue
- Le taux de livraison des paquets avec SUAP est proche de la solution de référence

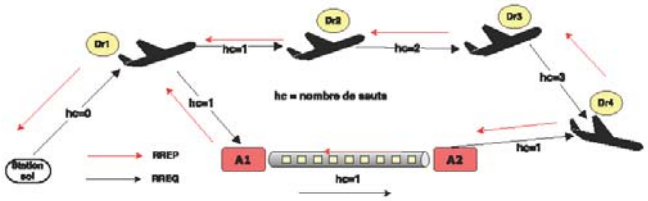




## Validation de la partition de sécurisation : évaluation des mécanismes contre l'attaque wormhole

**Test avec l'outil hybride**

## Validation des mécanismes contre l'attaque wormhole




| Paramètres | Valeur |
|---|---|
| Nombre de nœuds légitimes | 5 (4 drones et une station sol) |
| Mobilité | Rejoue de mobilité réelle |
| Protocole de routage | SUAP et AODV modélisé |
| Protocole MAC | 802.11 |
| Durée de simulation | 600 s |





## Contributions

### Génie logiciel

- Élaboration et validation d'une méthodologie de développement de systèmes embarqués critiques
- Utilisation de modèles pour concevoir l'architecture détaillée du système
- Vérification formelle des modèles et du code source généré

### Systèmes embarqués

- Implémentation d'un protocole de routage sur architecture ARM pour UAANET
- Mise en œuvre d'un réseau UAANET réaliste

## Contributions

**Sécurité des réseaux UAANET**

- Élaboration et validation du protocole SUAP
- Nos résultats valident que SUAP authentifie les messages et protège contre l'attaque wormhole
- SUAP offre un niveau de service équivalent au protocole AODV de référence

**Ingénierie système d'une flotte de drones**

- Prise en compte de la sûreté de fonctionnement
- Contribution à la certification d'un système UAS



## Plan de la présentation

- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
- **Conclusion**

## Security vs Safety

- L'impact des problèmes de "security" en aéronautique **est devenu autant si ce n'est plus important** que les problématiques historiques de "safety"
- **Traiter de façon disjointes** ces deux composantes d'un même système final n'a **plus de sens** à l'heure actuelle !
- Le monde "ouvert" (i.e. Internet) a intégré cette notion et **parle maintenant de besoin opérationnel**
  - Par opposition à besoins de "safety" ou besoins de "security"
- Les nouveaux **projets aéronautiques** (ex. SESAR, SESAR2020) intègrent maintenant la notion de "security for safety" dans leur analyse de risque



## Security for Safety : illustration sur un scenario d'attaque

- La perte d'un système IFE suite à une attaque d'un passager par l'intermédiaire du domaine POD (Passenger Owned Device) n'est pas un scenario qui doit être pris en compte dans le cadre des besoins de "security for safety"
- Par contre, la prise en main d'un IFE par un attaquant à bord qui permettrait par rebond de passer dans un autre domaine plus critique (ex. ACD – Air Control Domain) doit être pris en compte au titre de la "security for safety"

## Vers un standard d'analyse de risque

- Une méthode aéronautique est en train de voir le jour dans le cadre d'un groupe de travail de **l'EUROCAE, WG 72 "aeronautical security"**
- Cette méthode fortement inspirée de l'ISO 27000 permettrait de **concilier les aspects "safety", "security" mais aussi "security for safety"**
  - La difficulté d'une telle méthode réside dans la **traduction en niveau de "safety" d'une attaque visant initialement la "security"**
  - *Publication de la norme par le groupe de travail EUROCAE courant 2016*



## De nouvelles thématiques à considérer

- Problématique de la **certification des UAV/UAS**
- Intégration dans le **NAS (National Air Space) des UAS**
- **Security for Safety unifiée** pour l'ensemble du système ATM