Aircraft Security

Overview of the Aircraft Security Process

January 2019

Summary

- Threat Outlook
- Airbus Obligation and Duties
- Security Development Process & Security Assurance
- Security Risk Assessment
- Securing an information system
- Evaluate an Information System
- Conclusions

Summary

- Threat Outlook
- Airbus Obligation and Duties
- Security Development Process & Security Assurance
- Security Risk Assessment
- Securing an information system
- Evaluate an Information System
- Conclusions

AIRCRAFT SECURITY

THREAT OUTLOOK

Non exhaustive list

PHYSICAL SECURITY

Aircraft misappropriation (seizure) for blackmail purpose or for using it as mass destruction weapon (ex : 9/11)

Contamination of crews and passengers with **CBRN** agents

Unruly passenger, Hijacker, Terrorist

Electromagnetics Interferences (Impulses – Jamming)

Laser Illuminations

Ground attack (Bomb, missile…)

Aircraft **ground attacks** (ManPADS, lasers, drones,…)

Outstation

Operations & Dispatch centre

Gate

Aircraft **sabotage** on ground (unsecured aircraft vicinity / Insiders)

Improvised Explosive Devices (IED) on board (or incendiary devices)

Maintenance & Engineering Centre

Hangar

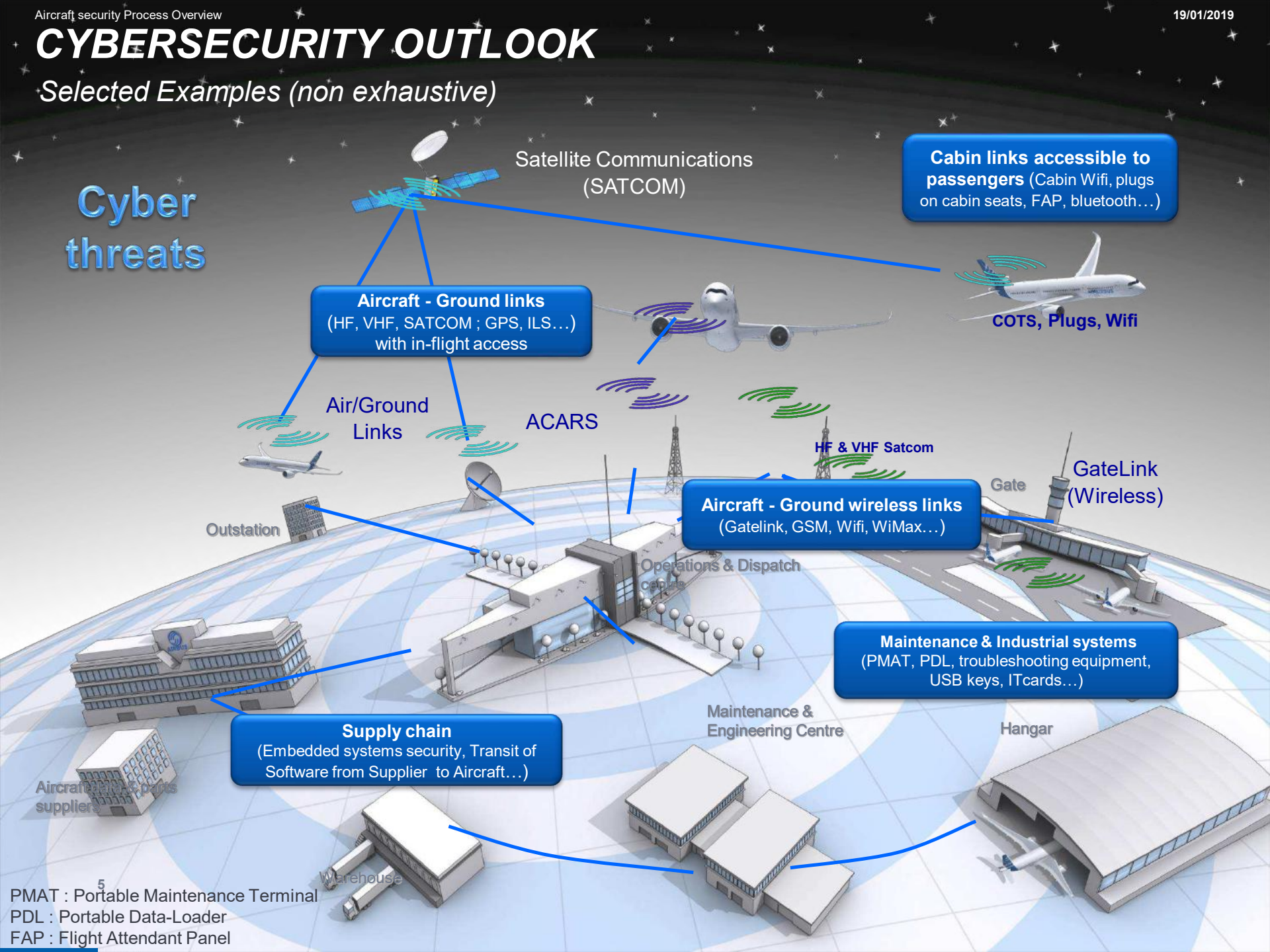
Aircraft data & parts suppliers

Warehouse

AIRBUS

CYBERSECURITY OUTLOOK

Selected Examples (non exhaustive)



PMAT : Portable Maintenance Terminal
PDL : Portable Data-Loader
FAP : Flight Attendant Panel

The e-enabled aircraft

Simple
Proprietary
Obscure
Isolated
Closed

Complex
Standardized
Documented
Connected
Open

An evolution of capabilities…but technology can be taken hostage

- ~144 Millions of new malwares samples recorded in 2014 (not specific to avionics software)
  - 12 millions per month
  - 400.000 per day
    - ➔ 4.5 new malware variant **every second !!!**

Aircraft Security Scope and Threats panorama

The reasons of fears…

CONNECTIVITY

Increased passenger connectivity

Increased real-time data to operate the A/C

Better prediction and reactiveness for improved safety and aircraft operation

Non time-critical data Performance analysis and big-data

Better prediction of performance trends for sustained aircraft operation

USAGE OF COTS

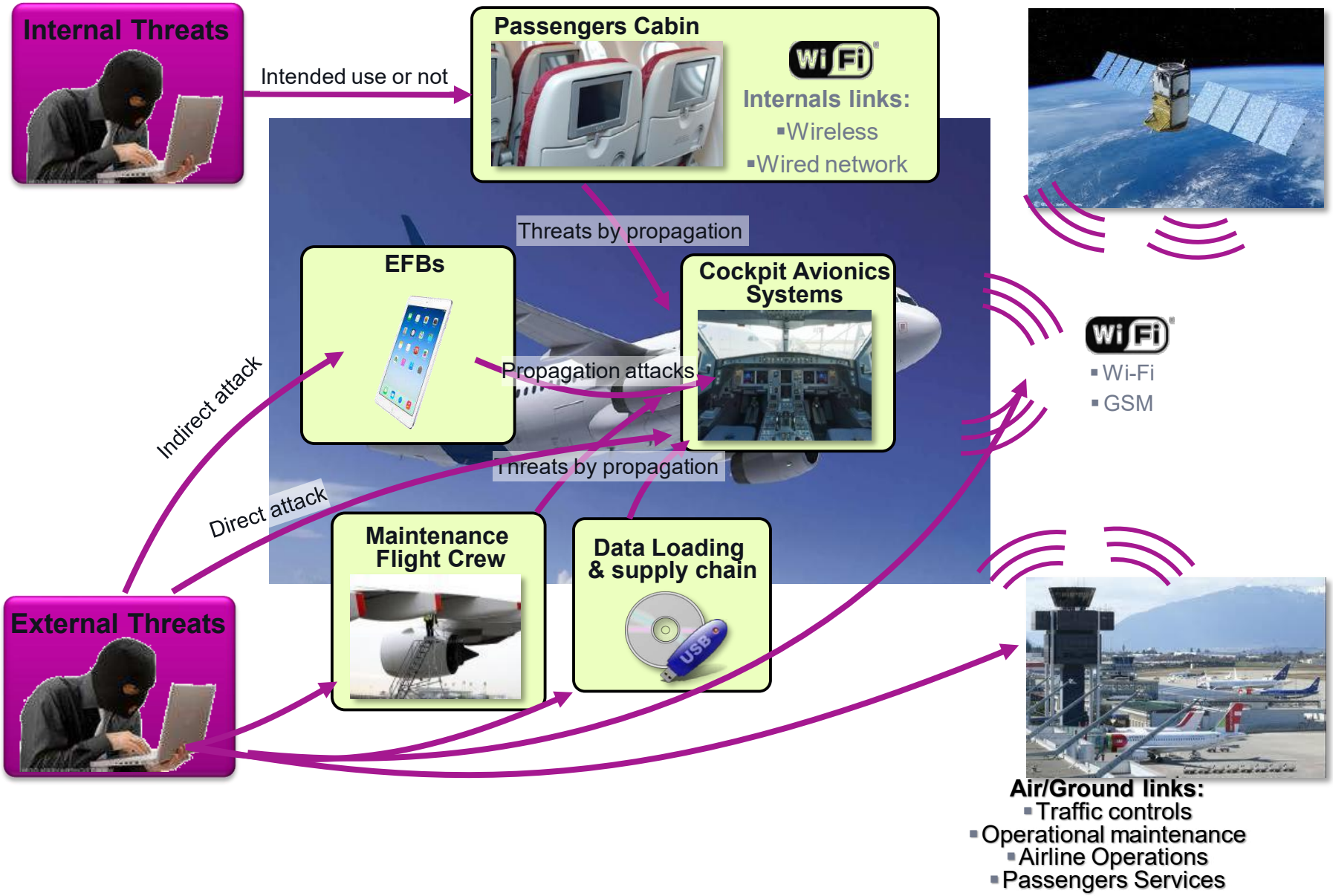
Extensive use of connectivity is all the more worrying that, at the same time, **economical constraints** pushes the community to use General Public Commercial Of The Shelf (GP-COTS) products to support the connectivity needs.

Aircraft Security Scope and Threats panorama

From a cyber point of view, an aircraft is : More than one thousand applications, dozens interconnected computers, dozen of operating systems Wi-Fi, Bluetooth, internet connections, USB keys... BUT…

… **No Security administrator on-board**

Considered Aircraft Exposed Interfaces



Aircraft Security scope and Threat panorama

Hugo Teso case

Aircraft Security scope and Threat panorama

Some examples Cabin connexion

Summary

AIRBUS & Aircraft Security : some keywords

- Started after 2001 with cockpit door reinforcement
- IT security concerns increased for the A380 EIS in 2006

- Airbus has built strong competences & knowledge around physical & IT security

- Our way of working : Anticipation
  - Analyse threat evolution & new technologies *(Aircraft intrusions, EMI, Drones, laser …)*
  - Security screening of events *(Airbus occurrences follow-up)*
  - Screening of Airbus modifications *(USB H/W on avionics for trouble shooting, new interfaces)*
  - Systematic risk analysis for new developments *(e.g FOMAX with Security Assurance Level application)*
  - Vulnerability management for COTS involved in new aircraft systems
  - Numerous intrusion testing by selected external bodies *(including government agencies)*

    Dataloaders, EFB, IPCOM, CABIN, ACARS, specific Avionic H/W, manufacturing, A/C Pen tests with ANSSI, BSI (=German ANSSI) , NSCS UK

  - Information to customers *(Security Information Bulletins, Security handbook)*
  - Development of security functions with Counter Terrorism Unit (eg: GIGN) *(A380 GSP, A350 AVIS, CVMS, …)*
  - Participation to International working groups
  - Cooperation with authorities

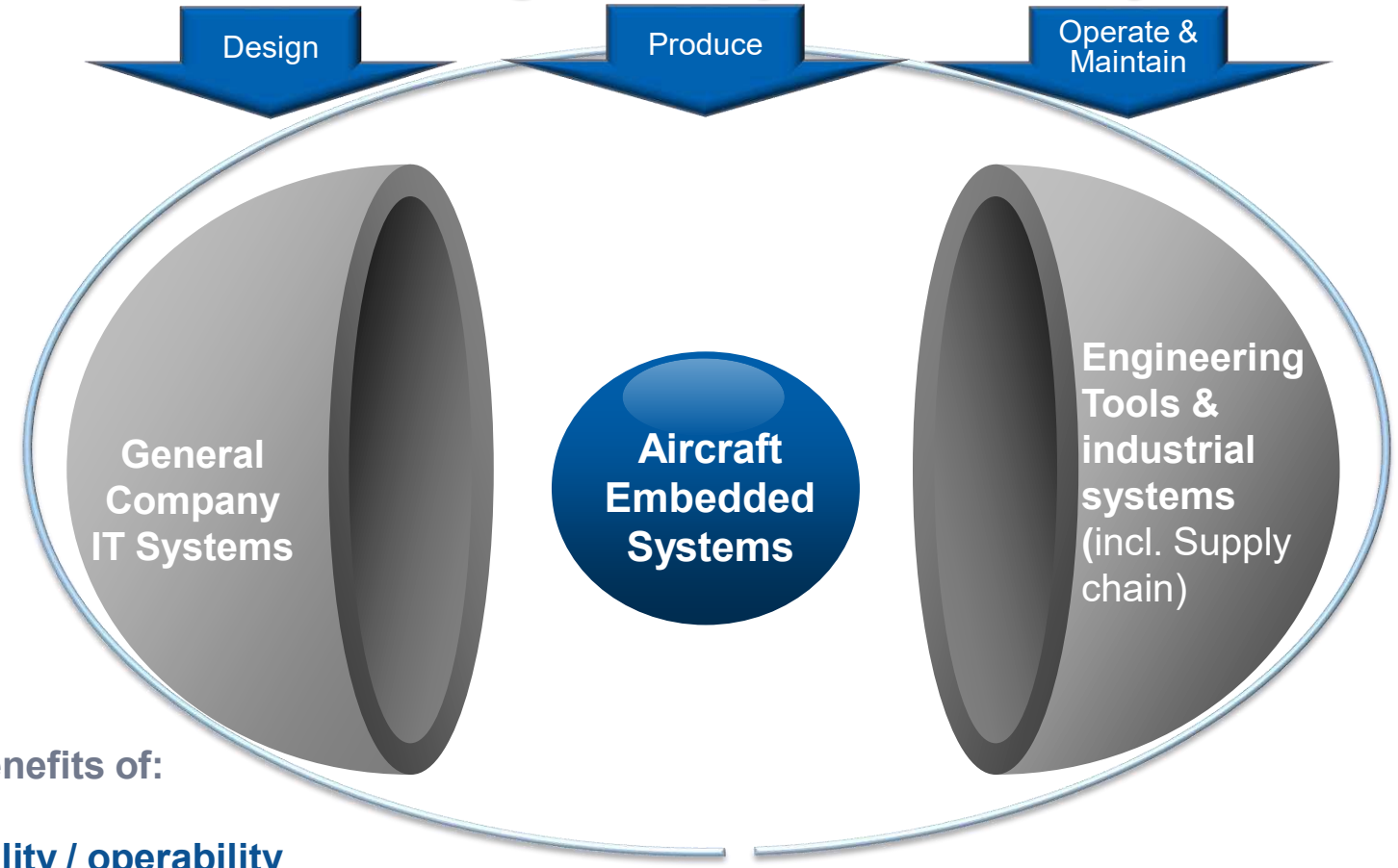
Safety Vs Security

Design Secure | Produce Secure | Maintain Secure

Aircraft manufacturer's obligations and Duties

Airbus' security in a nutshell…

Protect the Aircraft against Cyber Security Threats



For the benefits of:

- **Safety**
- **Reliability / operability**
- **Image / reputation / branding**
- **Passengers own devices**

Aircraft manufacturer's obligations and Duties

Obligations by regulation

- To ensure the certification of aircraft, the manufacturer has to comply with the rules regarding :

1. **DOA** (Design Organization Approval)

Design Secure

   - To provide reports and certify that the design of an aircraft, equipment or any part thereof or modification or repair schemes complies with authorities' requirements.

2. **POA** (Production Organization Approval)

Produce Secure

   - To ensure that the aircraft production complies with authorities' requirements until the aircraft delivery.

3. **TC Holder** (Maintain Security level)

Maintain Secure

   - To ensure that the aircraft security level is maintainable during commercial operations and support operators' activities.

Design Secure

Aircraft manufacturer's obligations and Duties

Reminder of the Regulatory Framework

Within the DOA, the main Aircraft Security activities are :

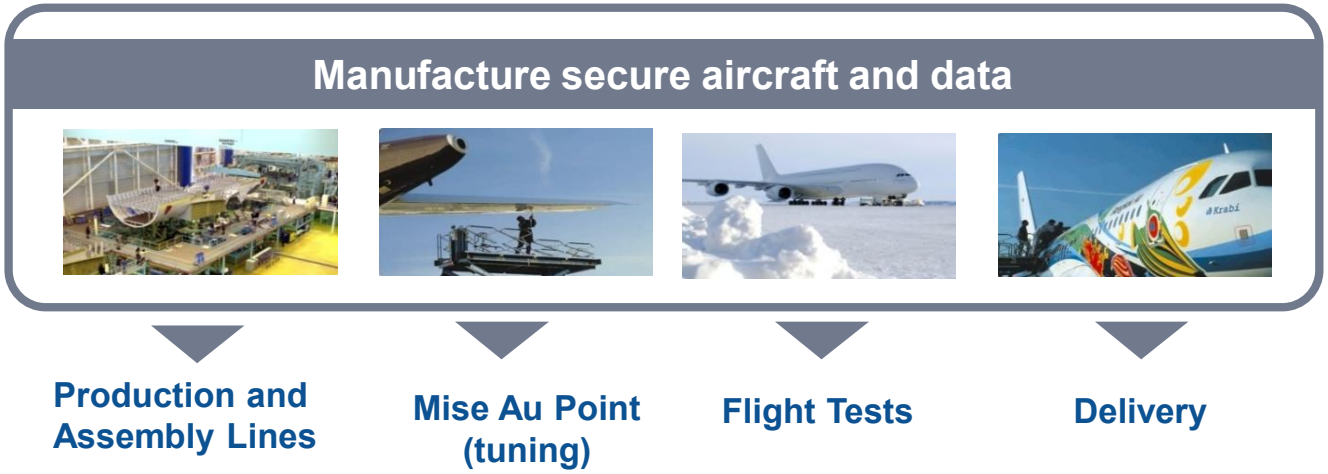
- Identification and evaluation of the threat and attackers (type & level)
- Agreements with programmes on the aircraft protections profiles
- Development of secured architectures and associated security functions
- Evaluation of Security effectiveness
- Assessement of compliance with existing security regulations
  - CRI F21 + CRI F47 For A380
  - CRI F38 For A350
  - CRI F119 For A320/A330
- Preparation of in-service aircraft operation (continued airworthiness)
- Accept the residual risk (100% secured doesn't exist) !

Produce Secure

Aircraft manufacturer's obligations and Duties

Regulatory Obligations for Airbus **POA**

After the design phase and prior to secured delivery to customer the aircraft has to be produced securely :



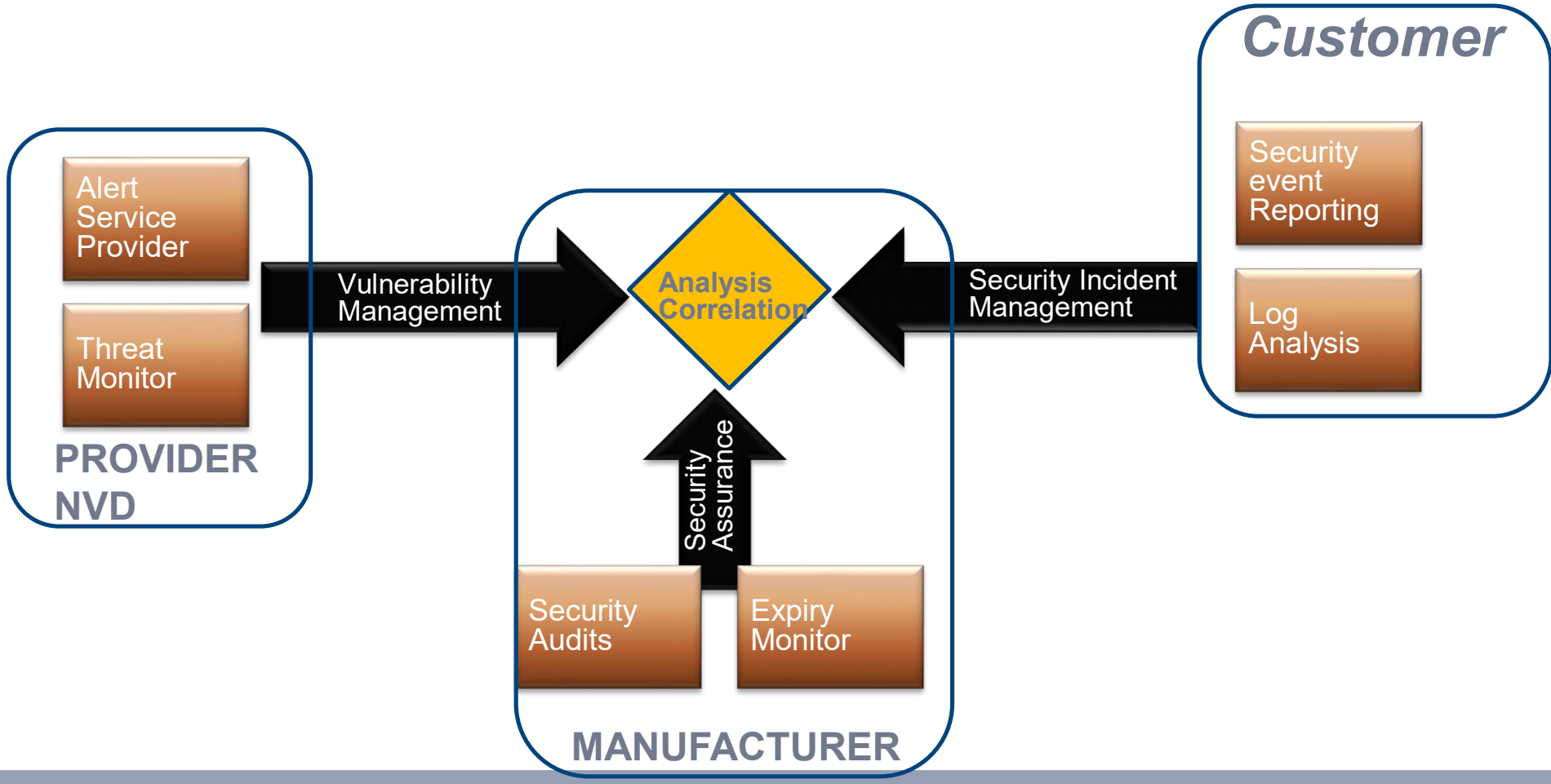
- Ensure aircraft security during **industrial activities**
- Ensure that the aircraft will reach its **performances**
- Ensure that **flight tests** activities will be performed in secure conditions
- Ensure that the aircraft will be **delivered secure**

Design Secure

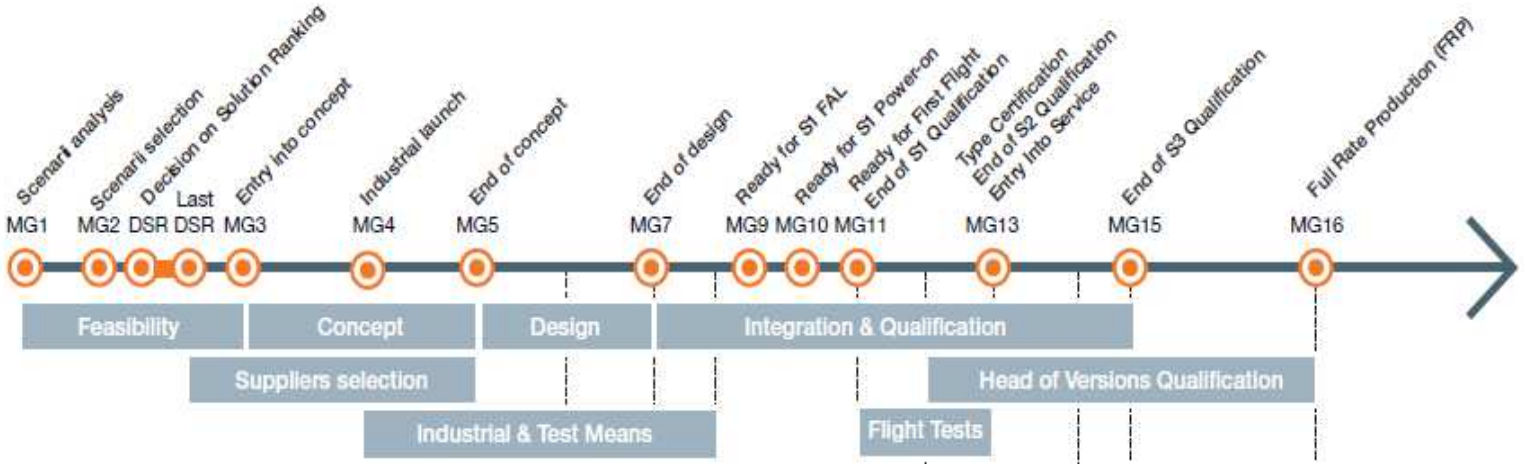
Maintain Secure

Aircraft manufacturer's obligations and Duties

Regulatory Obligations for **TC Holder**



Plan for product development (PDP)
Aircraft security is fully part of it



Security Plan

Security Context

Security Context

A/C Functional Impact Analysis

MS/Syst. Functional Impact Analysis

Security Handbook

A/C Specification

MS/Syst. Specifications

A/C Verification

MS/Syst. Verification

A/C Security Risk Assessment

A/C Security Risk Assessment

MS/Syst. Security Risk Assessment

Industrial Security Manual

MS/Syst. Security Risk Assessment

Security measures

Security measures

Risk treatment Plan

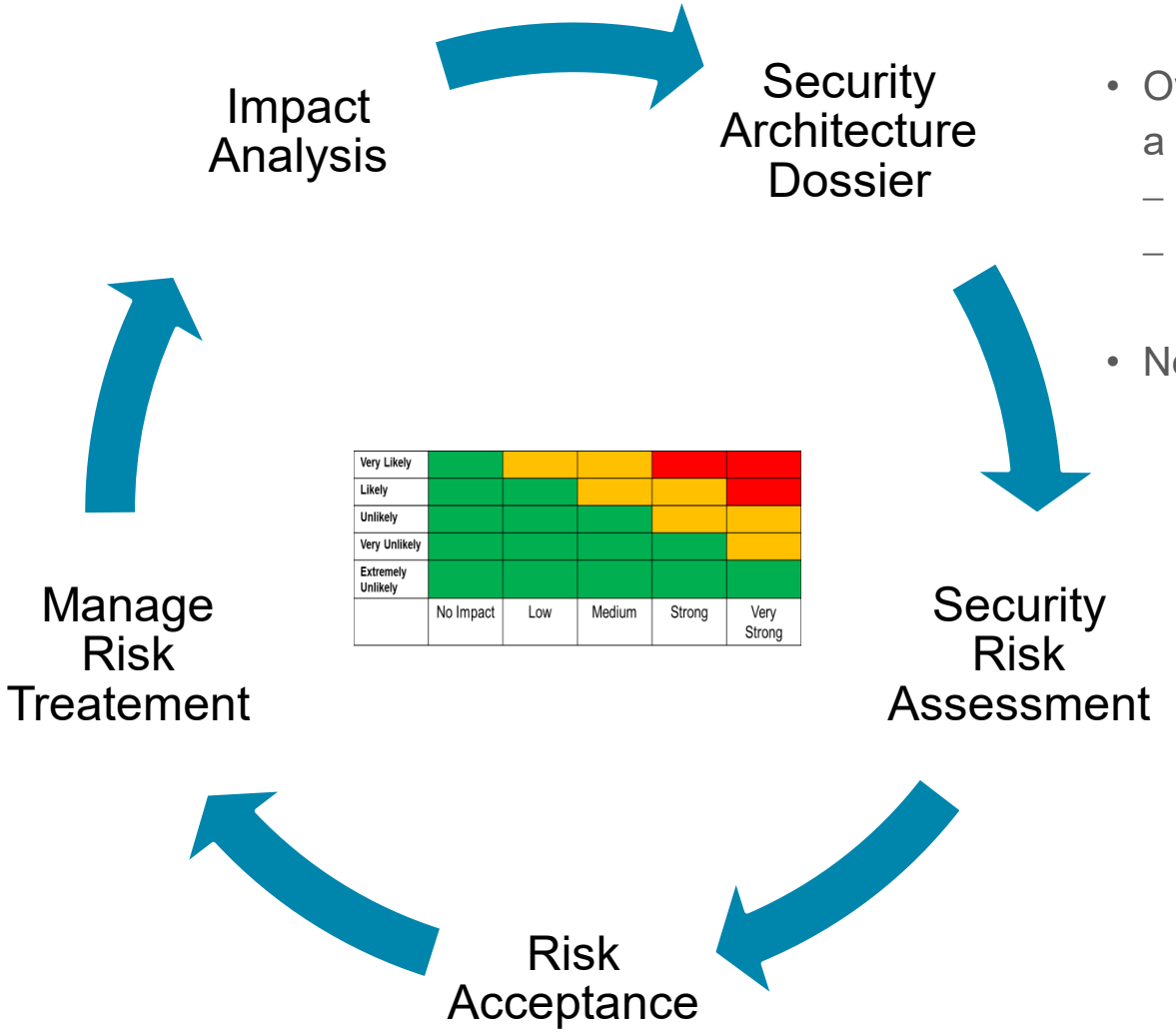
Risk treatment Plan

Main security deliverables in PDP

Summary

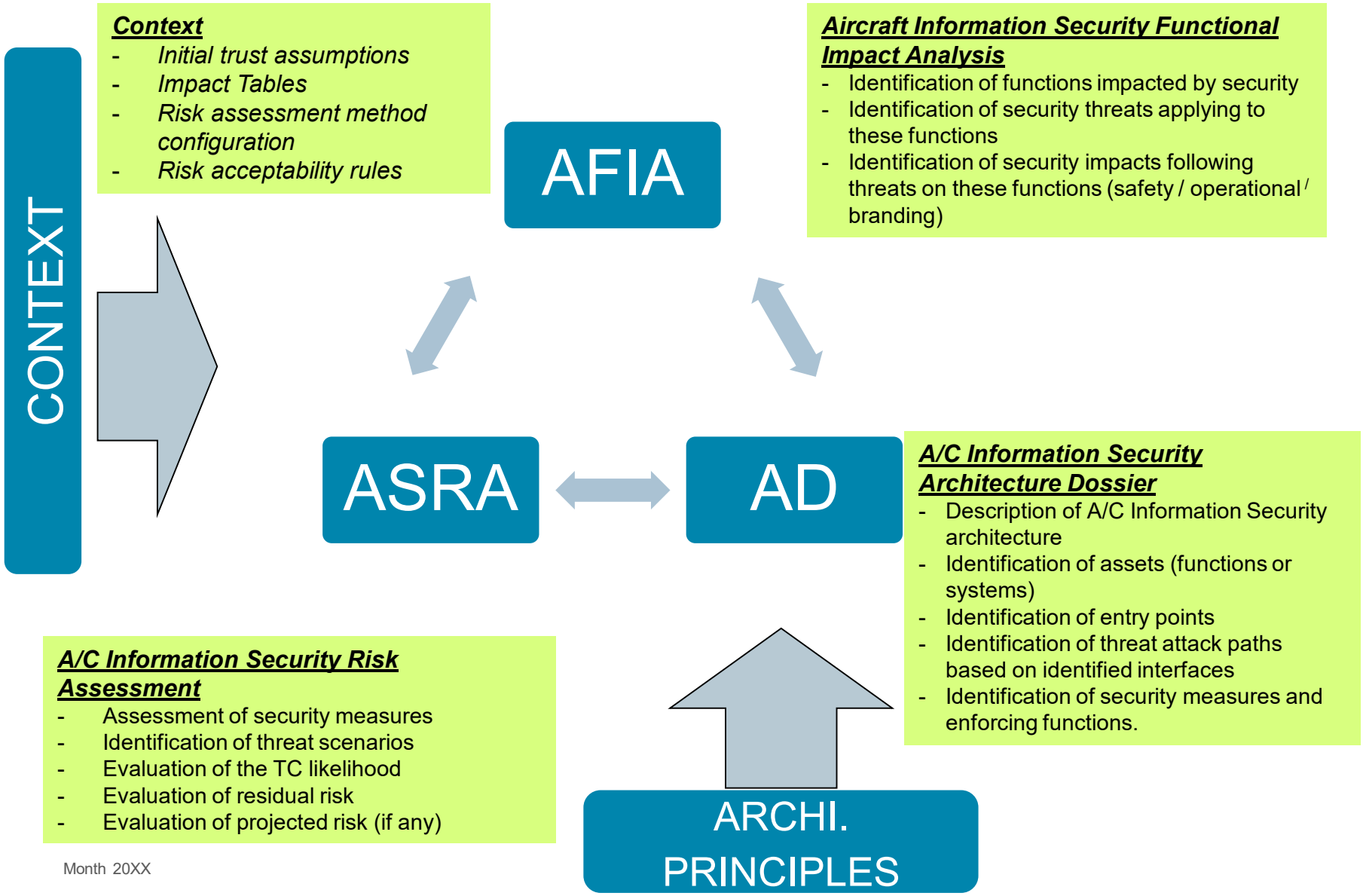
- Threat Outlook
- Airbus Obligation and Duties
- **Security Development Process & Security Assurance**
- Security Risk Assessment
- Securing an information system
- Evaluate an Information System
- Conclusions

Overall Information Security Process



- Overall Information Security Process is a Risk Based Approach
  - Probability of an attack is 100%
  - 100% secure does not exist !
- Need to assess the risk of an attack vs
  - Potentiality (Likelihood)
  - Impact

Introduction to Context / AFIA / AD / ASRA / Archi. Principles



A/C Information Security Context defines:

- **Initial Trust Assumptions**
  - ie: Pilot is not a threat source / Maintainer is not a threat source / Passenger is a threat source
  - ie: Aeronautical service provider is not a threat source. (ex: ARINC / SITA)
  - Ie: Aeronautical signals are not a threat source (ex: ILS / GPS / GNSS / VOR / ADF / DME / Weather Radars)
  - Ie: Aeronautical equipment supplier is not a threat source
  - Ie: Transport is a threat source.
- **Defines Public and Private zones**
  - ie: Cabin is public / threat source.
  - ie: Avionics bay is private / not a threat source.
  - Ie: Wireless networks reachable in public zone are publicly accessible / threat source
- **Defines risk assessment methodology**
  - M20667.1 based on ED-203 & ISO 27001
- **Defines Security Impact Levels and Tables**
  - Eg: What does mean a STRONG security impact vs Safety ? Operations ?
- **Requests for Security Assurance Demonstrations in new development including:**
  - Vulnerability management.
  - No malicious code introduced

A/C Information Security Functional Impact Assessment

- ***AFIA Key Inputs:***
- A/C Context
- Functional breakdown
- A/C FHA / SSA
- SFIA (System Functional Impact Analysis)
- ORA (Operational Risk Analysis)
- Cockpit Effects

Aircraft Security: Security Impact vs Safety Effect

Security Impact	Safety Consequences as per 25.1309	Other Safety Consequences
VERY STRONG	Failure Condition triggered by a threat having safety consequences assessed **CATASTROPHIC**	○ Safety consequences triggered by a threat having: -On occupants excluding flight crew: Multiple fatalities. -On flight crew: Fatalities or total incapacitation consequences
STRONG	Failure Condition triggered by a threat having safety consequences assessed **HAZARDOUS**	○ Safety consequences triggered by a threat having: - On aeroplane: Large reduction in functional capabilities or safety margins, - On occupants excluding flight crew: Serious or fatal injury to a small number of passengers or cabin crew - On flight crew: Physical distress or excessive workload impairs ability to perform tasks • Serious or fatal injuries to people on ground (A/C stationary).
MEDIUM	Failure Condition triggered by a threat having safety consequences assessed **MAJOR**	○ Safety consequences triggered by a threat having: - On aeroplane: Significant reduction in functional capabilities or safety margins, -On occupants excluding flight crew : Physical distress, possibly including injuries -On flight crew: Physical discomfort or a significant increase in workload • Injuries to people on ground (A/C stationary)
LOW	Failure Condition triggered by a threat having safety consequences assessed **MINOR**	○ Safety consequences triggered by a threat having: -On aeroplane: Slight reduction in functional capabilities or safety margins, -On occupants excluding flight crew: Physical discomfort On flight crew: Slight increase in workload
NO IMPACT	No effect	No effect

Aircraft Security: Security Impact vs Operational Effect

Security Impact	Definition for Airline Flight, Ground, and Maintenance Operations
VERY STRONG	Event that has a fleet level impact: Fleet unavailable due to Type Certificate suspension, airline self-imposed fleet grounding (for example severe hacking event confirmed…)…
STRONG	Event that potentially generates a high operational severity delay: RTG, RTO, IFTB, a diversion, cancellation, an increase in flight crew workload, a severe disturbance of passengers' comfort, a high disturbance of the traffic on airport or ATC, an impossibility to dispatch as per the SOP and MMEL procedure in a standard environment or route. Event that potentially generates additional aircraft downtime than planned: Out phase SBs, AD, MEL repair....
MEDIUM	Event that would generate a medium operational severity delay: Additional flight or cabin crew workload as procedure deviates from standard operating procedure but not leading to a RTG, RTO, IFTB or diversion, event with an impact on the standard dispatch process in terms of tools needed, ground support, coordination between maintenance/flight ops/airport, coordination with ATC...
LOW	Event that would generate a low severity delay, i.e. below 15min.
NO IMPACT	Event with no impact on aircraft operations: Event with no effect to the flight crew, no maintenance effect that can be reported in the technical logbook

A/C Architecture Dossier

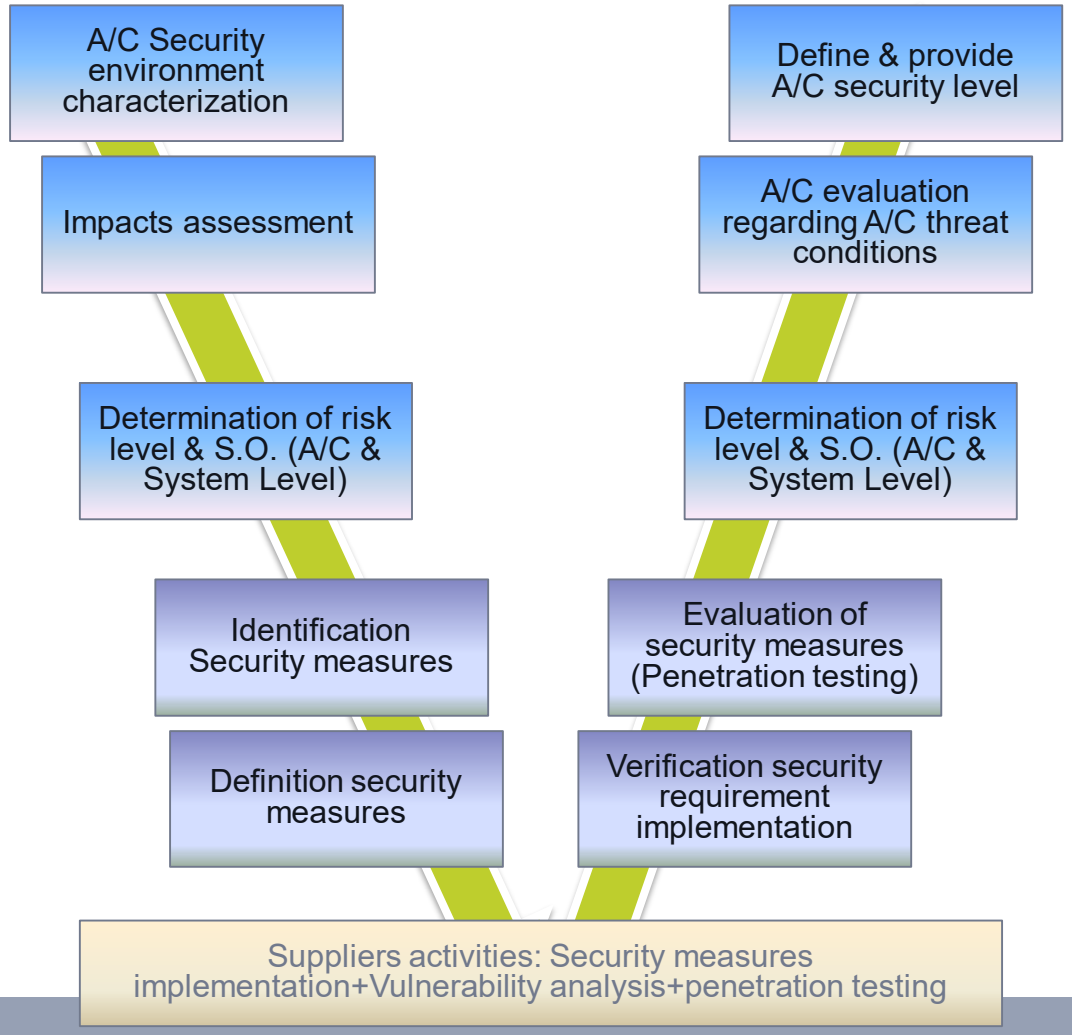
- ***AD Key Inputs:***

- *Std Specs*
- *Configuration catalogs*
- *Configuration in service*
- *FCOM / MMEL*
- *AFIA*
- *SIDs*
- *SDD*
- *Technical notes*
- *Wiring documents*
- *Audit results*

A/C Security Risk Assessment

- ***ASRA Key Inputs:***
- *Interfaces*
- *Threat conditions*
- *Threat Attack paths*
- *Security Measures*

Aircraft security development process



Aircraft security development process

- Top-down of the process permits to:
  - Define and validate the security requirements from the aircraft level down to the item or equipment level according to risk identification,

- Bottom-up of the process permits to:
  - Verify that the security requirements have been correctly and completely addressed and implemented in the aircraft design according to risk mitigation needs,
  - Evaluate implemented security measures at aircraft and system level through penetration testing,
  - Determine residual risks once the security measures are implemented in the design through security risk analysis at system level (SSRAs) and aircraft level (ASRA, DSRAs).

Conclusion (1/2)

- The Security development process allows:
  - To attain a level of **confidence in the aircraft security level**
  - **To control residual risks**
    - Identified, assessed, mitigated, accepted
    - During the whole aircraft lifecycle
  - To attain a level of confidence in the **demonstration process of the security level**
  - **To provide a formalization of Security activities**
  - To establish **security evidence** towards Airworthiness Authorities

Conclusion (2/2)

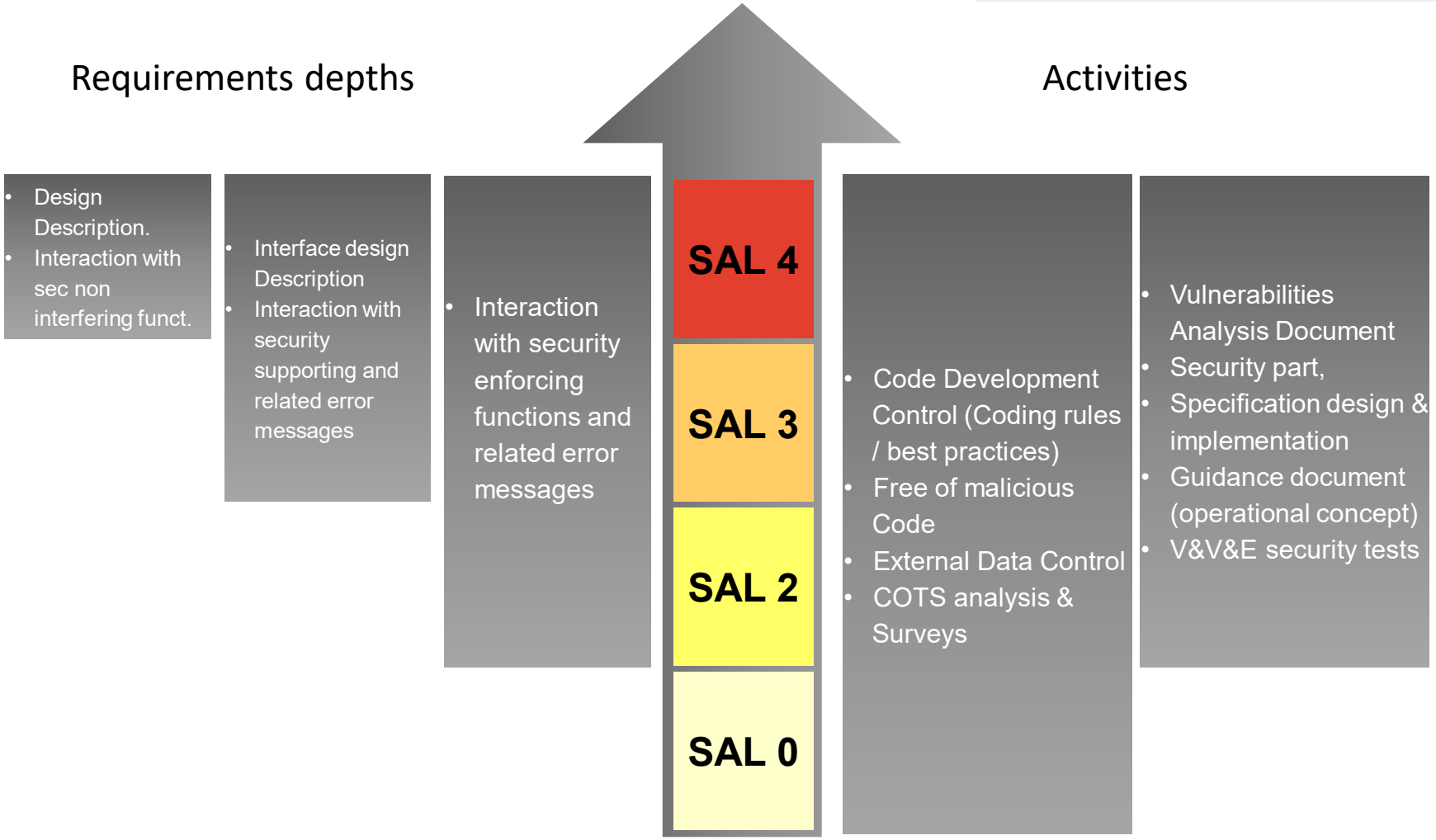
- **Risk based approach allows:**
  - To **design a secure Aircraft Information System**

*Risk analysis drives the **Aircraft Information System Security Architecture** and the way the **Security Measures** are integrated into systems*

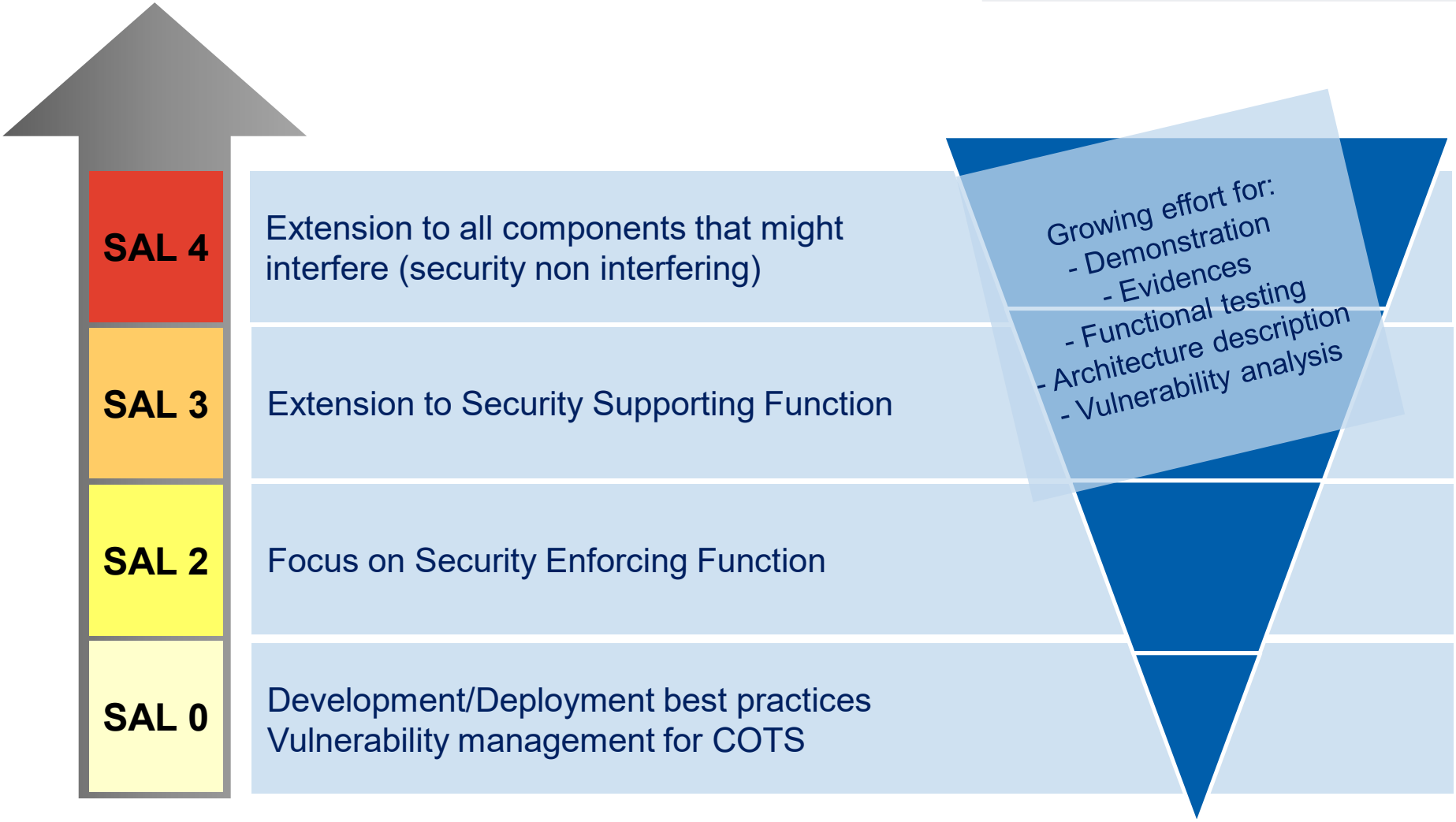
  - To **demonstrate that residual security risks are managed**

Risk assessment drives validation, verification and evaluation at System level and for the whole Aircraft Information System

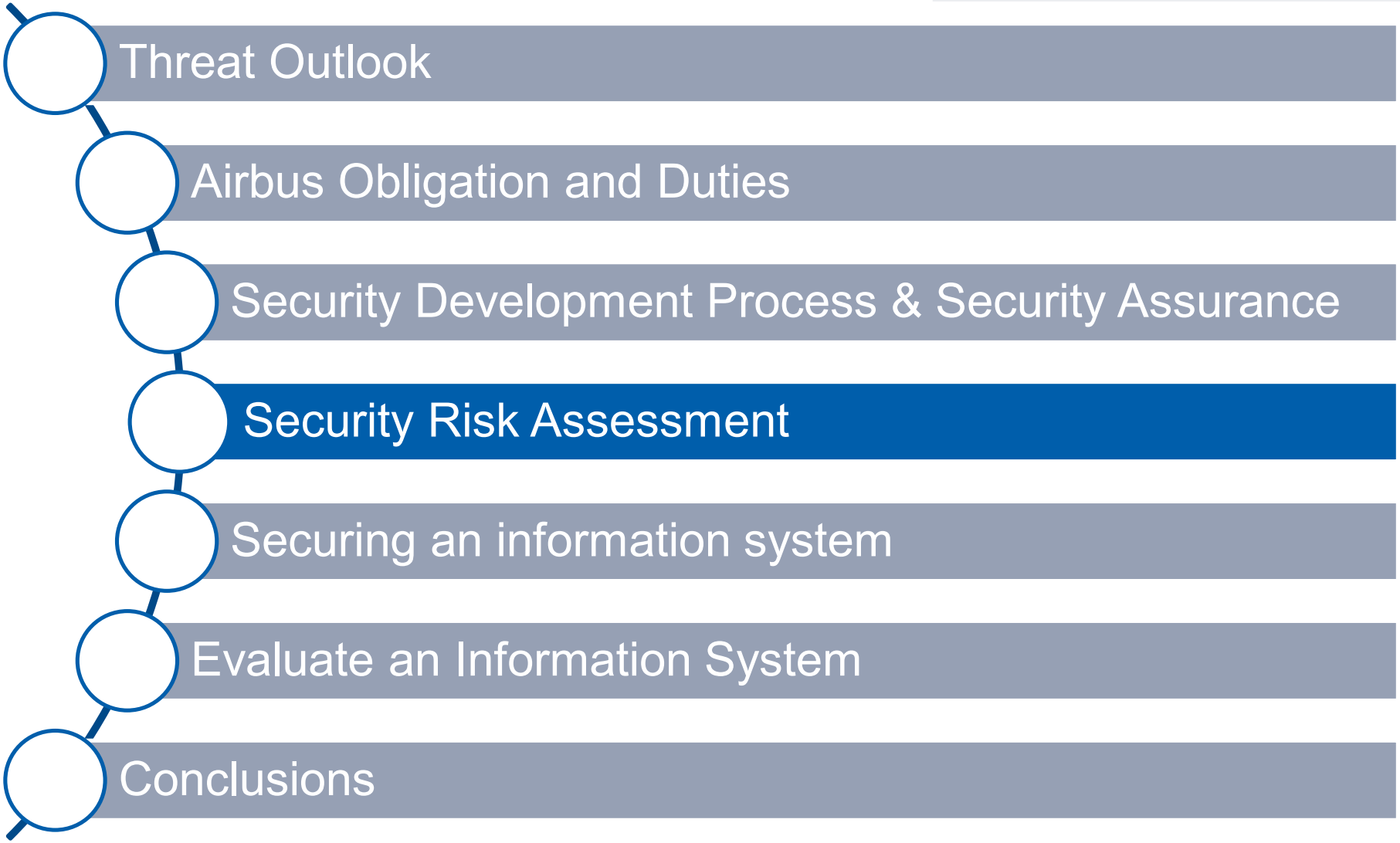
Security Assurance Levels



Security Assurance Levels / effort



Summary

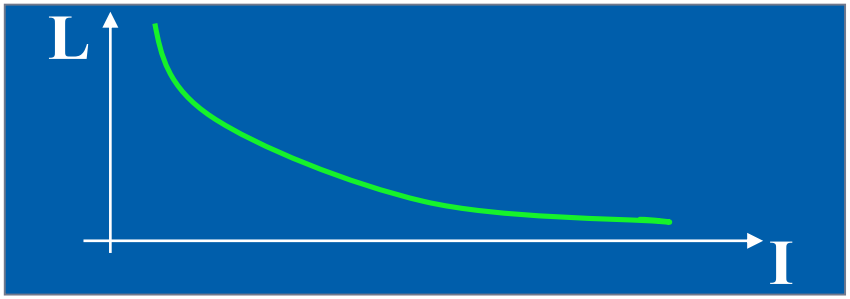


Definitions

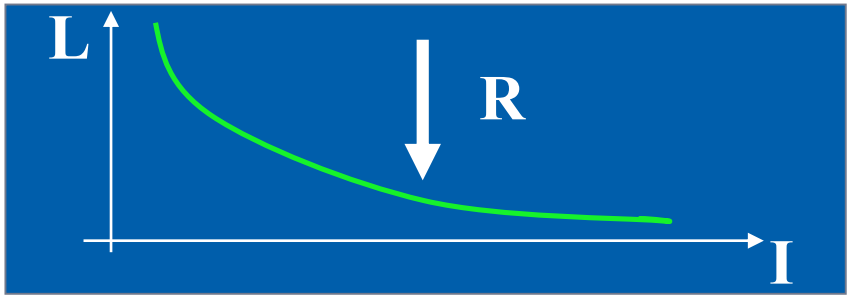
CONCEPT	Definition
Target of Risk analysis	Item (IT system, function, product…) which is subjected to risk evaluation
Asset	Everything and everybody you put value in (hardware, software, doc, etc)
Threat (Attack)	Any potential violation of security that could cause direct or indirect damages to an asset, if it was occurring.
Threat scenario	Potential causal chain / sequences of actions that could be performed to accomplish a threat
Vulnerability	Weakness in an asset (information system, system security procedures, internal controls, or implementation) that could be exploited or triggered by a threat source to lead an attack
Risk	The combination of the potentiality and the impact of a threat to arise
Threat Potentiality	Qualitative indication of the likelihood of a threat scenario to occur
Threat impact	Qualitative indication of the criticality of the effects of a threat.
Intrinsic Threat Potentiality & impact	Qualitative indication of potentiality and impact without taking into account any security measure
Security Objective	High level requirement expressing a security need and allowing to decrease a risk to an acceptable level.
Security measure	Any action, device, procedure, or organizational and technical measure that reduces the potentiality and/or the impact of threats

Aircraft Security: Focus on Risk Assessment

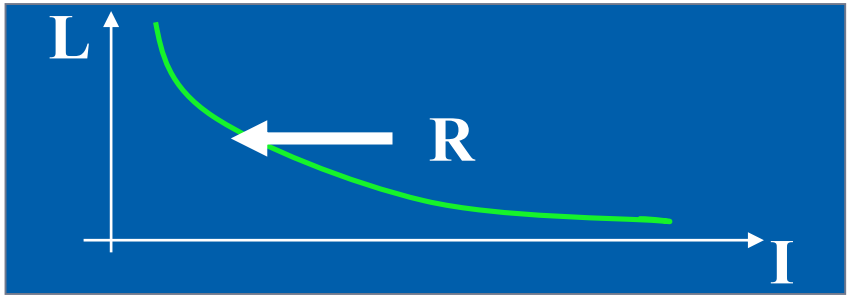
$$Risk = f(Likelihood, Impact)$$



Prévention



Protection



Security Risk Assessment – Based on internal method (derived from ED-203)

$$Risk = f(Likelihood, Impact)$$

The risk is as much high as attacking the target represents a stake for the aggressor.	Attacker Motivation
The risk is as much high as the aggressor has the feeling that he takes no risk for himself (impossibility to get back	Attacker Impunity
The risk is as much high as the conditions of emergence are easy to prepare	Preparation Means
The risk is as much high as the time window to perform the attack is wide	Window of Opportunity
The risk is as much high as there are low measures to protect against the attack	Execution Means

Security does not only mean "**injuries & death**", a lot of others assets have to be considered :

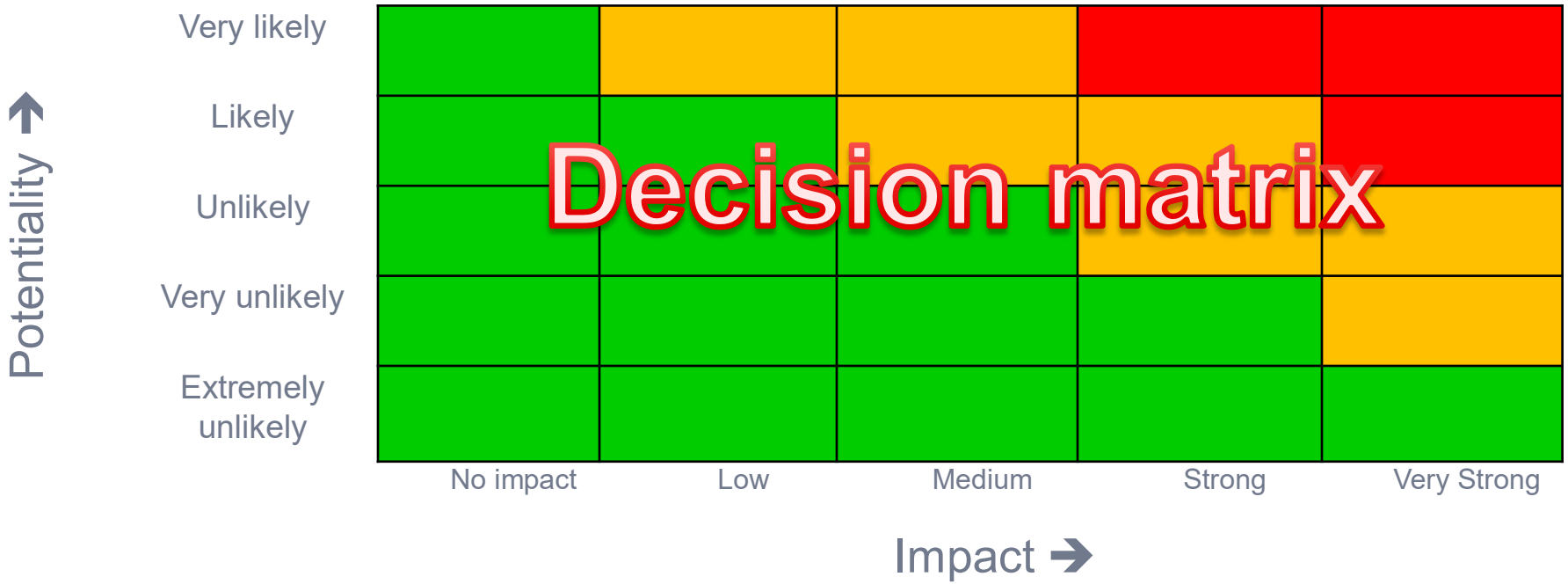
1. Aircraft Safety
2. Dispatch reliability and aircraft operation (business)
3. Airbus and Customers commercial image, trust and reputation
4. Passenger personal assets
5. Others…

Aircraft Security: Focus on Risk Assessment
Vraisemblance (Likelihood)

- Possibilité que quelque chose se produise. La vraisemblance peut être définie, mesurée ou estimée objectivement ou subjectivement, ou avec des termes descriptifs généraux (tels que rare, improbable, possible, certain), sous formes de fréquence ou de probabilités mathématiques (ref: British Standard 25999-1:2006)

	Potentialité
5	Very Likely
4	Likely
3	Unlikely
2	Very Unlikely
1	Extremely Unlikely

Aircraft Security activities - Security risk assessment



Methodology for identifying THREATS and building THREATS SCENARIOS

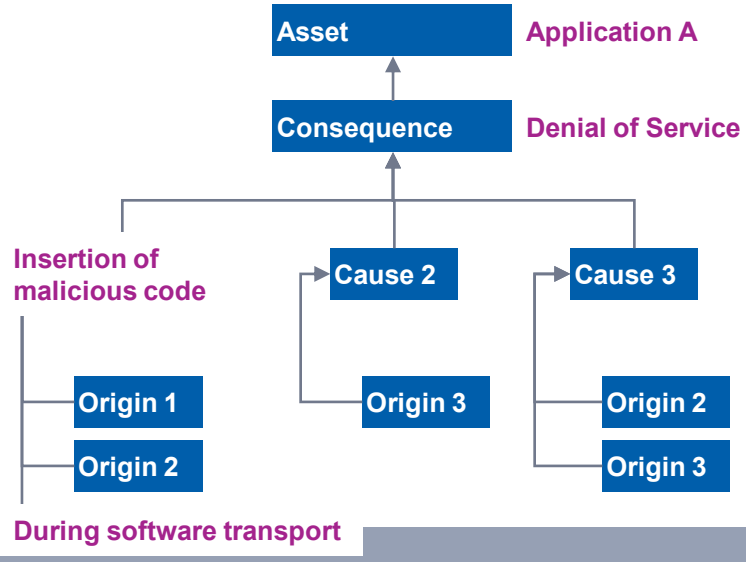
- To study the risks concerning a system, the identification of the potential events which may harm the system has to be led.

  ⇒ This task is accomplished by **identifying threats and threat scenarios** applicable to the system.

A threat is a potential attack targeting an asset.

A threat can be performed by several threat scenarios.

- **Each scenario** can be described by:
  - The **type of resources** targeted by the scenario (asset): data, function, equipment, etc.
  - The **type of consequence**: Corruption, loss, disclosure, etc.
  - The **types of cause** being able to lead to this situation of risk: Malicious code introduction, source code modification, etc.
  - The **origins of the scenario**, where this scenario is performed: in suppliers environment, during media transport, via wireless communication link, etc…



Likelihood: Security Measures and Their Effect

Goal: Identification of all Risk Reduction Factors

Fundamental paradigm:

Everything is a security measure!

- If it reduces the likelihood of an attacker succeeding, it is a security measure
- No matter whether it is (not exhaustive)…
  - …a dedicated technical function
  - …a technical function already found in the basic system design
  - …a technical function identified through another process (e.g. safety)
  - …an operational procedure suggested by us or already present
  - …pre-conditions to be met like…
    - …availability of information & equipment
    - …accessibility of interfaces
    - …necessary knowledge

The terms "security measure" and "countermeasure" are used interchangeably

Likelihood: Security Measures and Their Effect

- Security measure effect is based on a scale from 1 – 30
- In practice, it will usually be 1 – 10 (depending on factors to be explained)
- High number → highly effective
- Even minimum effect 1 does reduce the likelihood, however

Final likelihood is the result of a series of reductions based on countermeasures

Goal: Identification of all Risk Reduction Factors

Likelihood: Reduction Factors

Goal: Consistent, Reproducible, Realistic Assessment

- Each “security measure” (i.e. an aspect reducing the likelihood) has an evaluated effect
- Usually, this effect ranges from 1 – 10
  - Exceptions are possible
  - Any value can be given with appropriate rationale (e.g. diode has higher effect)
- Measures are classified according to their effect in three phases:

1. Preparation Means

Will the attacker need to acquire specific knowledge?

Will she need to acquire/prepare specific equipment?

2. Window of Opportunity

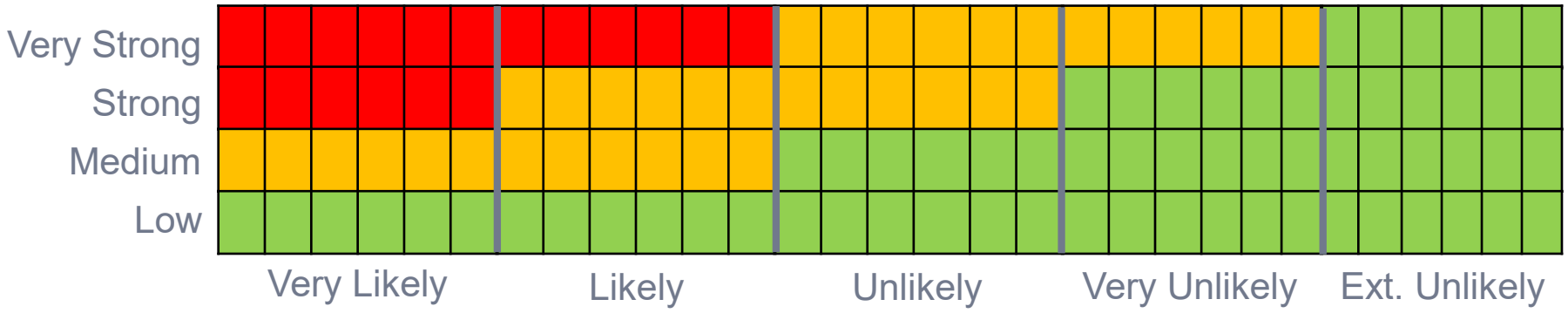
Does this measure limit the exposure of the external interface used to attack?

3. Execution Means

Which skills/equipment etc. will the attacker need to carry out the attack?

Risk Grid

Very Likely	Low	Low	Medium	High	High
Likely	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Low	Medium	Medium
Very Unlikely	Low	Low	Low	Low	Medium
Extremely Unlikely	Low	Low	Low	Low	Low
	No Impact	**Low**	**Medium**	**Strong**	**Very Strong**

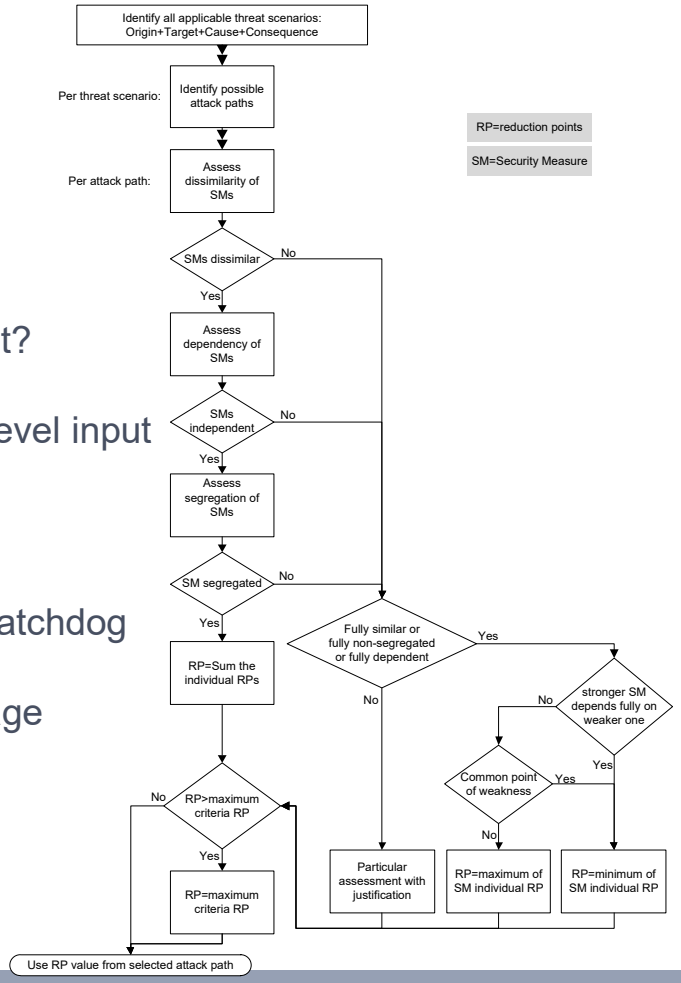


Likelihood: Combined Effectiveness

“So I have these two security measures each worth 5 points…”

Goal: Consistent, Reproducible, Realistic Assessment

- How much do I reduce? 5 points? 10 points? Something in between?
- It depends on:
  - **Dissimilarity**
    - Are the two conceptually and technologically different?
    - Counter example: two iptables firewalls
    - Positive example: layer 3/4 firewall plus application level input verification
  - **Independence**
    - Is one needed to make the other work?
    - Counter example: deactivation switch triggered by watchdog process
    - Positive example: authentication function and message signature
  - **Segregation**
    - Can they be taken out in one step?
    - Counter example: shared kernel
    - Positive example: two physical boards



Likelihood: Effectiveness Capping

Goal: Consistent, Reproducible, Realistic Assessment

There is a finite limit to effectiveness…

- If the attacker has already spent three months preparing, will another month really stop her?
- Likewise, if the attacker has already gone through five technical barriers, will the sixth one really be a problem?
- Does it make a difference whether there is five minutes or one minute to carry out the attack?

Sum of security measure effect is limited per factor:

Criterion	Maximum Combined Reduction
Preparation Means	6
Window of Opportunity	8
Execution Means	18

Likelihood/Risk: Attacker Profile

“Who would want to try this anyway?”

Goal: Separate Attack Attempt from Execution

- This depends on **motivation (only)**! Not skill, expertise etc.
- SMs aim to stop the execution. Attacker profile assesses precondition.
- Motivation linked to attacked asset
  - Safety impacts without risk for attackers personal safety
  - Safety impacts including risk for attackers personal safety
- Attacker profiles
  - Untargeted malware attack, e.g. common worms or viruses as found on the Internet; these could be brought onto the Aircraft inadvertently. Due to the untargeted nature of the attack, this profile should only be considered for relatively low impacts.
  - Commercially motivated attacker (e.g. blackmailer, industrial spy, organized crime)
  - Terrorist and national intelligence services, national spies…

Residual risk level assessment

- **Final assessment:**
  - **After having identified Security objectives, risk level shall be re-assessed to check that risk level has been decreased to an acceptable level.**
  - **After having implemented Security measures, answering to security objectives, risk level shall be re-assessed to check that risk level has been decreased to an acceptable level.**

⇒ **These both analysis loops shall be repeated until the risk level is acceptable**

Likelihood: Putting it Together

Goal: Intuitively Readable Evaluation on One Page

	Outside Security Process		Inside Security Process		Effectiveness Capping
	Technical	Operational	Technical	Operational	
Preparation Means	SM1 (v)		SM3 (x)		$C_p = \max(e_r - 6, 0)$
Window of Opportunity		SM2 (w)			$C_w = \max(e_r - 8, 0)$
Execution Means			SM4 (y) SM5 (z)		$C_e = \max(e_r - 18, 0)$
Current Execution Likelihood	$L_{OT} = 30 - e_c$	$L_{OO} = L_{OT} - e_c$	$L_{IT} = L_{OO} - e_c$	$L_{IO} = L_{IT} - e_c$	$L = \max(L_{IO} + c, 1)$

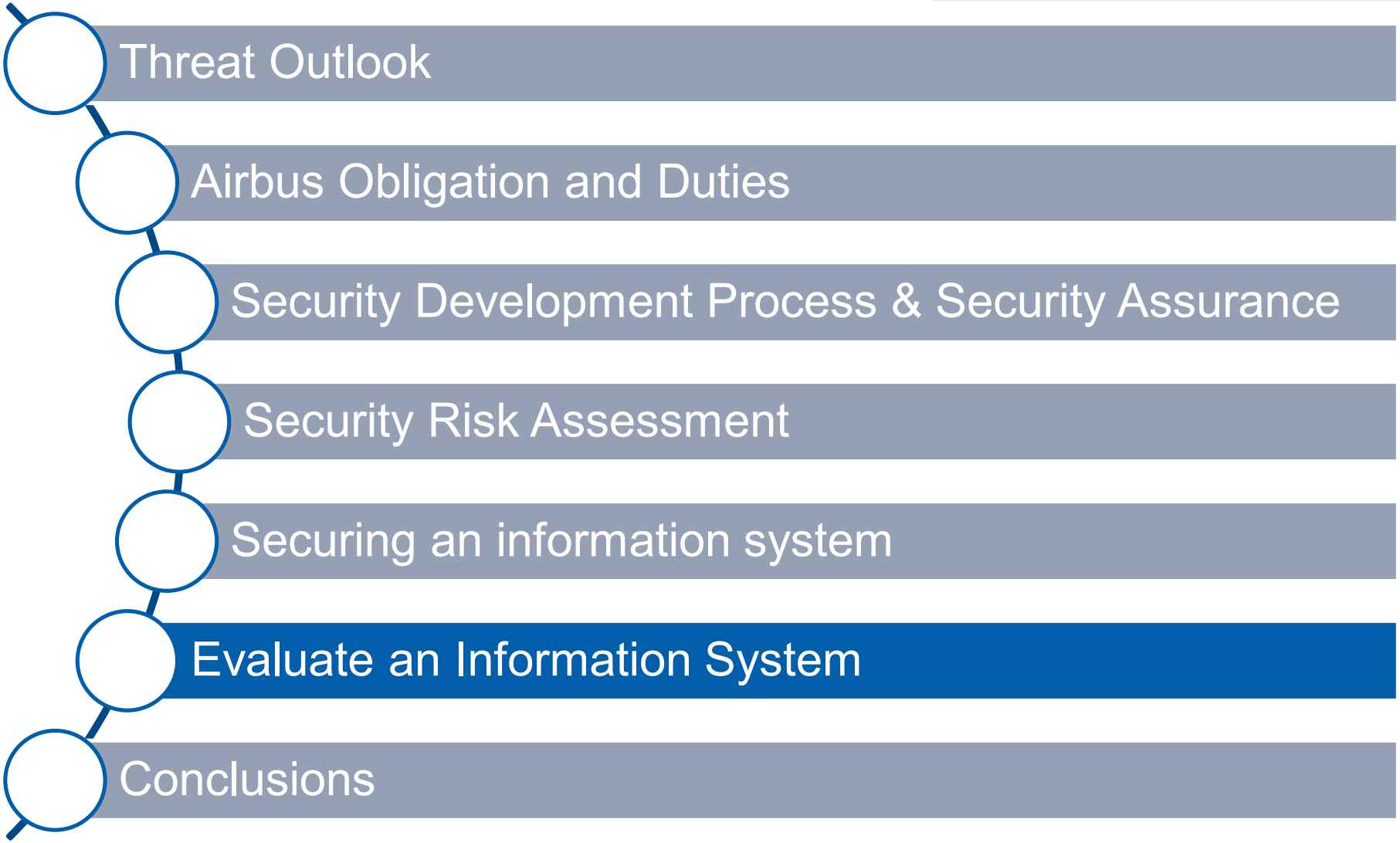
e: sum of row/column

“Inside”: Requirements identified through the security process (security is main stakeholder)
“Outside”: Security relevant things we found already there, i.e. defined through another process (somebody else is main stakeholder)

Summary

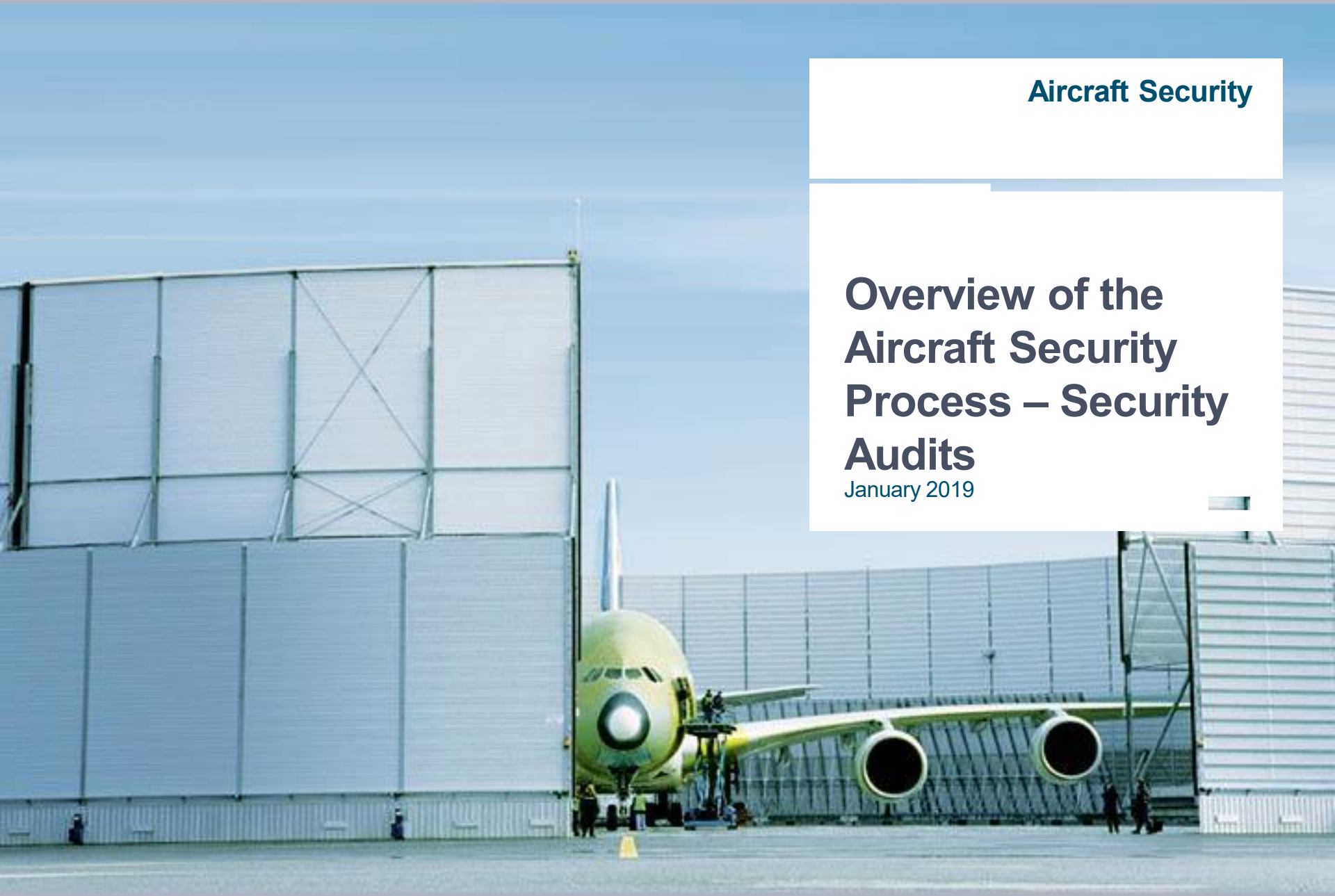
- Threat Outlook
- Airbus Obligation and Duties
- Security Development Process & Security Assurance
- Security Risk Assessment
- **Securing an information system**
- Evaluate an Information System
- Conclusions

Summary



Summary

- Threat Outlook
- Airbus Obligation and Duties
- Security Development Process & Security Assurance
- Security Risk Assessment
- Securing an information system
- Evaluate an Information System
- Conclusions



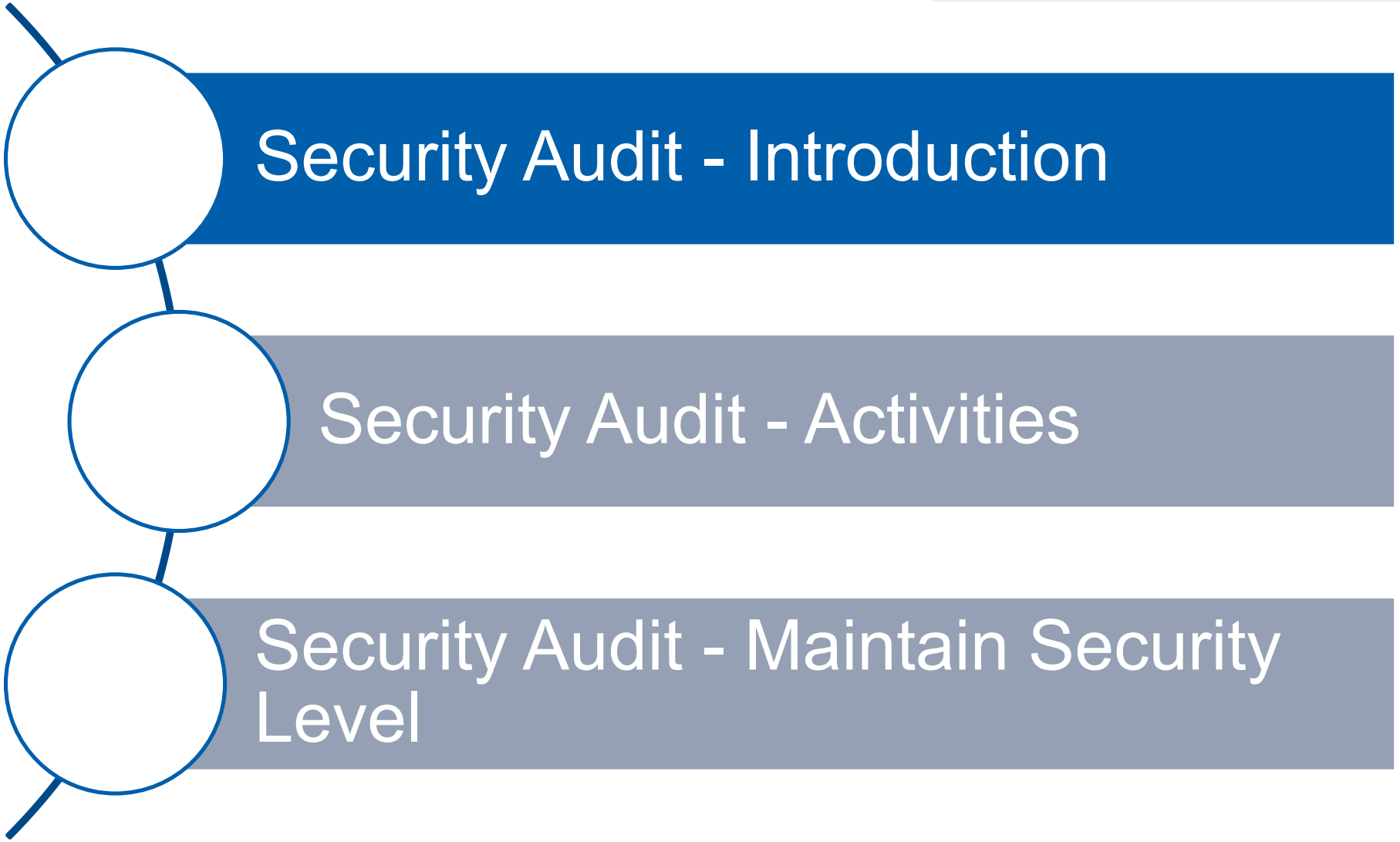
Aircraft Security

Overview of the Aircraft Security Process – Security Audits

January 2019

Summary

Summary



Audit de sécurité: Définition
Scenario d'attaque

- Attaque: Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, erreur de configuration, etc.) à des fins non connues par l'exploitant du système et généralement préjudiciables.

- Deux grands types d'attaque sur les réseaux :
  - Sur les protocoles de communications
  - Sur les applications standards (HTTP, SMTP, FTP…)

- Les motivations des attaques peuvent être de différentes sortes :
  - obtenir un accès au système
  - voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
  - glaner des informations personnelles sur un utilisateur
  - récupérer des données bancaires ;
  - s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
  - troubler le bon fonctionnement d'un service
  - utiliser le système de l'utilisateur comme « rebond » pour une attaque
  - utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

Préambule: Aspects légaux

- Pratique du reverse peut tomber sous le coup de la loi:
  - Sociéte Tegam vs. Guillermito, condamnation de Guillermito pour avoir “reversé” le logiciel de Tegam sans disposer de licence.
- Protection de l’information: il est essentiel que les documents, les outils, les résultats (ex.: vulnérabilités trouvées) soient protégés par un contrat (ex.: Non Disclosure Agreement: NDA).
- Il est important que les audits soient couverts par des contrats d’assurance spécifiques en cas de déterioration des équipements ou des pertes d’exploitation.
- …

Audit de sécurité: Définition
Attaque informatique

- Un scénario d'intrusion sur un système peut se décomposer en six actions élémentaires, enchaînées selon un processus itératif :

Renseignement
- Découvrir l'architecture du système, son plan d'adressage
- **Ecoute, furetage, espionnage, cryptanalyse**

Préparation
- Dégrader ou contourner la sécurité
- **Leurrage, sabotage, bombe logique, parasitage, saturation**

Intrusion
- Entrer par un point faible
- **Usurpation de nom, d'adresse, cheval de Troie, essais exhaustifs**

Installation
- Installer une entrée permanente
- **Porte dérobée, canal caché**

Camouflage
- Cacher l'entrée permanente
- **Cacher les répertoires et fichiers pirates, inhiber la surveillance**

Propagation
- Attaquer les machines ou systèmes en mutuelle confiance
- **Rebond IP ou X25, rhosts, domaines WinNT, virus, ver**

Audit de sécurité: Définition

- Black box audit

  The black box audit is considered as a penetration test. In this scheme, the auditor is located outside the environment to do his testing of the security features. This means that only user or externally accessible resources are viewed. The auditor may or may not have information regarding the evaluated feature, but any information he has will be basic. As everything is hidden to the auditor, he must discover details about the network by himself.

- White box audit

  The white box audit is sometimes referred as a manual audit. This audit type requires an onsite visit of the auditor and includes an examination of many aspects of the network security, resulting in a deeper determination of the security implementation than the black box audit. All information (documentation, source code, network topology,...) is provided to the tester. It requires a heavy workload and provides the most helpful test report.

Audit de sécurité: Définition

- Grey box audit

  A grey box audit is performed on all interfaces of a specific system. Documentation is available but limited. Source code is not provided or only for specific parts. The auditors penetrate a system using public known software or hacker techniques. The outcome is documented in a security report.

Audit de sécurité: Définition

- Fuzzing (test en frelatage): “is the process of sending intentionally invalid data to a product in the hopes of triggering an error condition or fault. These error conditions can lead to exploitable vulnerabilities.”
- Les entrées sont générées aléatoirement de façon à observer en sortie les cas d’erreur ou de plantage du programme, ce dernier cas sera analysé pour rechercher l’origine.

- Ex.: Google en 2011 a réussi par Fuzzing à trouver plus de 100 bugs dans le lecteur Flash d’Adobe. Il lui fallu analyser 20 téraoctets de fichiers SWF, pour en extraire 20000 fichiers ensuite utilisés pour la campagne de tests à l’aide de 2000 coeurs CPU.

Audit de sécurité: Définition

- Reverse engineering ou reverse (rétroconception): consiste à analyser un système de manière à pouvoir comprendre son fonctionnement interne et être capable de le reproduire.
- L'analyse peut se faire en boîte blanche de manière statique (en l'absence de toute exécution: désassembleur). Ou en dynamique à l'aide d'un debugger.
- L'analyse peut se faire en boîte noire de manière passive (capture réseau) ou active si on génère des données en entrée pour observer le comportement du programme en sortie.

Audit de sécurité: Exemple 1

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int check_authentication(char *password) {
   int auth_flag = 0;
   char password_buffer[16];

   strcpy(password_buffer, password);

   if(strcmp(password_buffer, "brillig") == 0)
      auth_flag = 1;
   if(strcmp(password_buffer, "outgrabe") == 0)
      auth_flag = 1;

   return auth_flag;
}

int main(int argc, char *argv[]) {
   if(argc < 2) {
      printf("Usage: %s <password>\n", argv[0]);
      exit(0);
   }

   if(check_authentication(argv[1])) {
      printf("\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-\n");
      printf("          Access Granted.\n");
      printf("-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-\n");
   } else {
      printf("\nAccess Denied.\n");
   }
}
```

- Que fait ce programme ?
- Quelle est la valeur de sortie du programme?
- Précisez en quoi est-il vulnérable?
- Comment peut-on analyser en détail son comportement?
- Quelle solution simple permettrait de le corriger?

Audit de sécurité: Généralités

- **Pourquoi faire un audit de sécurité**:
  - Anticipate incident/problem
  - Measure policy compliance
  - Threat environment evolves: Assessing risk & security level
  - Assessing potential damage
  - Change management
  - Security incident response
  - …

Audit de sécurité: Généralités

- **Quand faire un audit de sécurité:**
  - Emergency
  - Regulatory obligation
  - Before entry into service
  - Scheduled/maintenance
  - Design modification
  - …

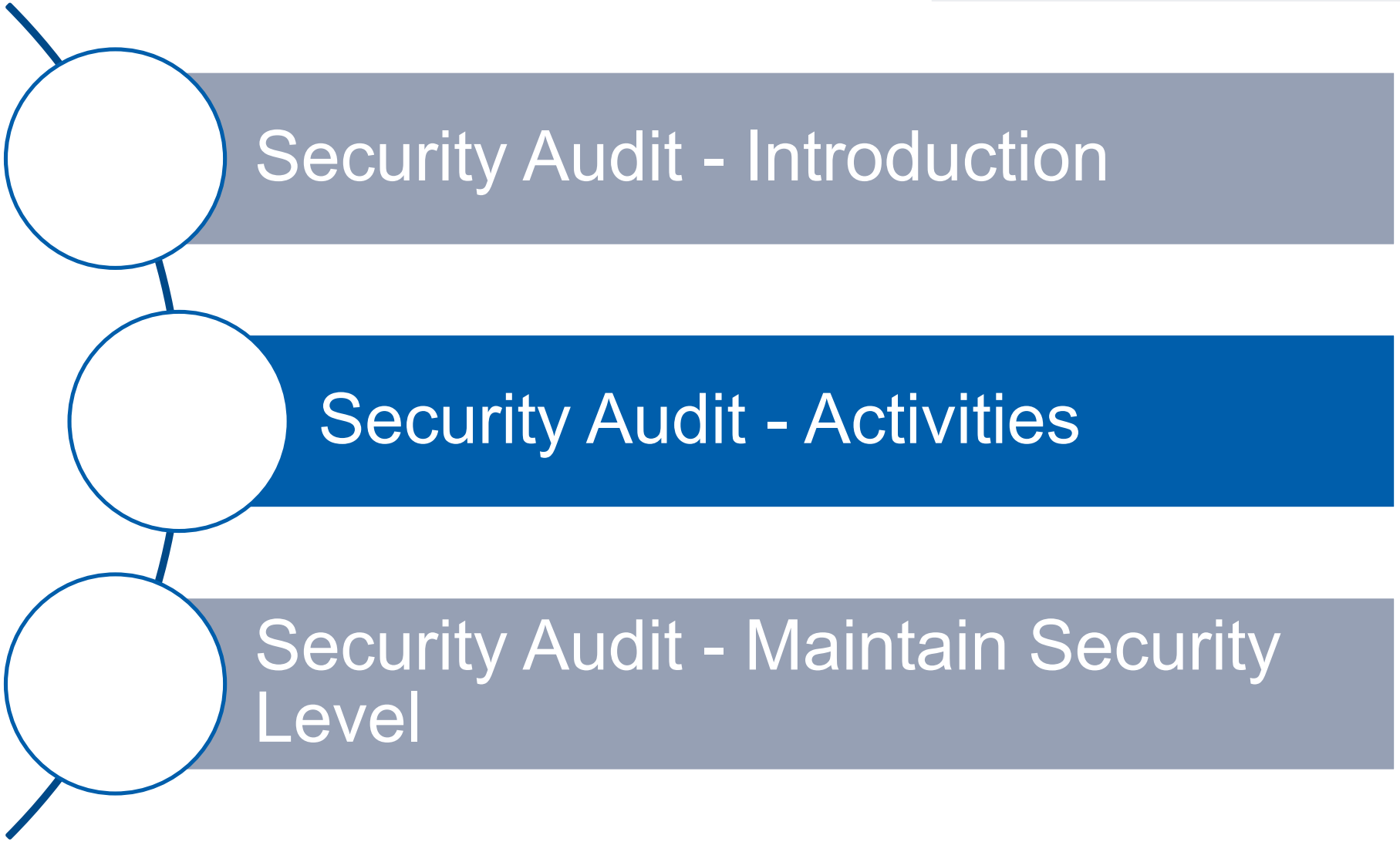
Audit de sécurité: Généralités

- **Fréquence des audits dépend du scope et du niveau d'exposition du système:**
  - Individual Host/system: 12/24 months
  - Large Networks: 12/24 months
  - Network: 12 months
  - Firewall 6 months
  - …

Audit de sécurité: Généralités

- **Comment faire un audit, les principales étapes:**
  - Preaudit: Plan & objectives
  - verify your tools and environment
  - Audit/review security policy
  - Gather audit information
  - Generate an audit report
  - Take actions based on the report's findings
  - Safeguard data & report

Summary



Activités d'audit et d'évaluation du système d'information bord

For onboard system different security audits and tests types can be performed:

- ✓ Development tests
- ✓ Integration tests
- ✓ MOCK-UP tests
- ✓ Assembly Line & maintenance tests
- ✓ Flight tests

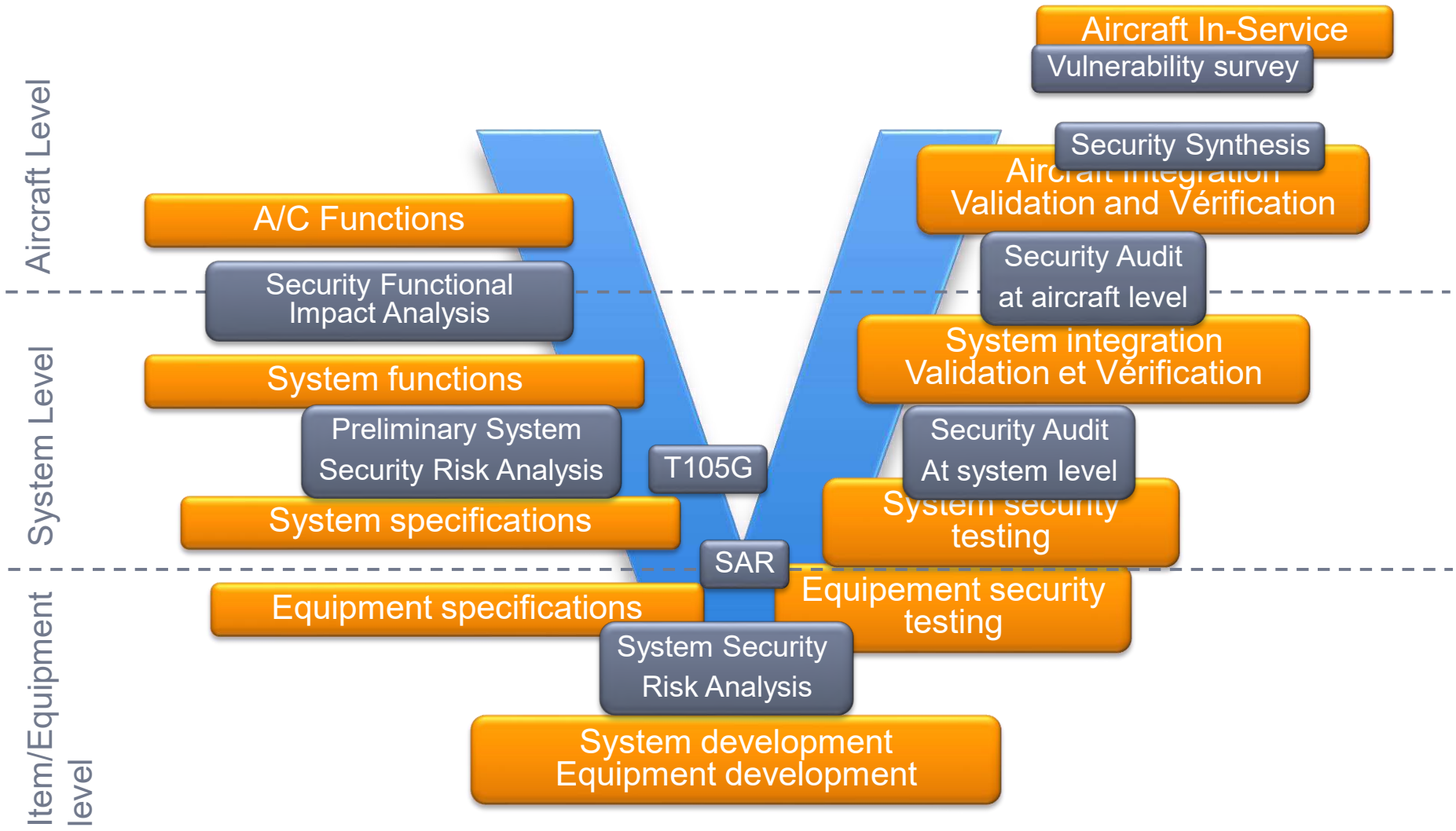
These tests categories can be split in more detailed parts like:

- ✓ Development tests on software at the supplier facilities
- ✓ Integration tests on system benches (System integration/functional integration)
- ✓ Higher level of integration tests based on MOCK-UP like V&V Platform
- ✓ Software loading tests and maintenance tests in the Final Assembly Line
- ✓ Ground tests & fight tests on an almost integrated

Activités d'audit et d'évaluation du système d'information bord

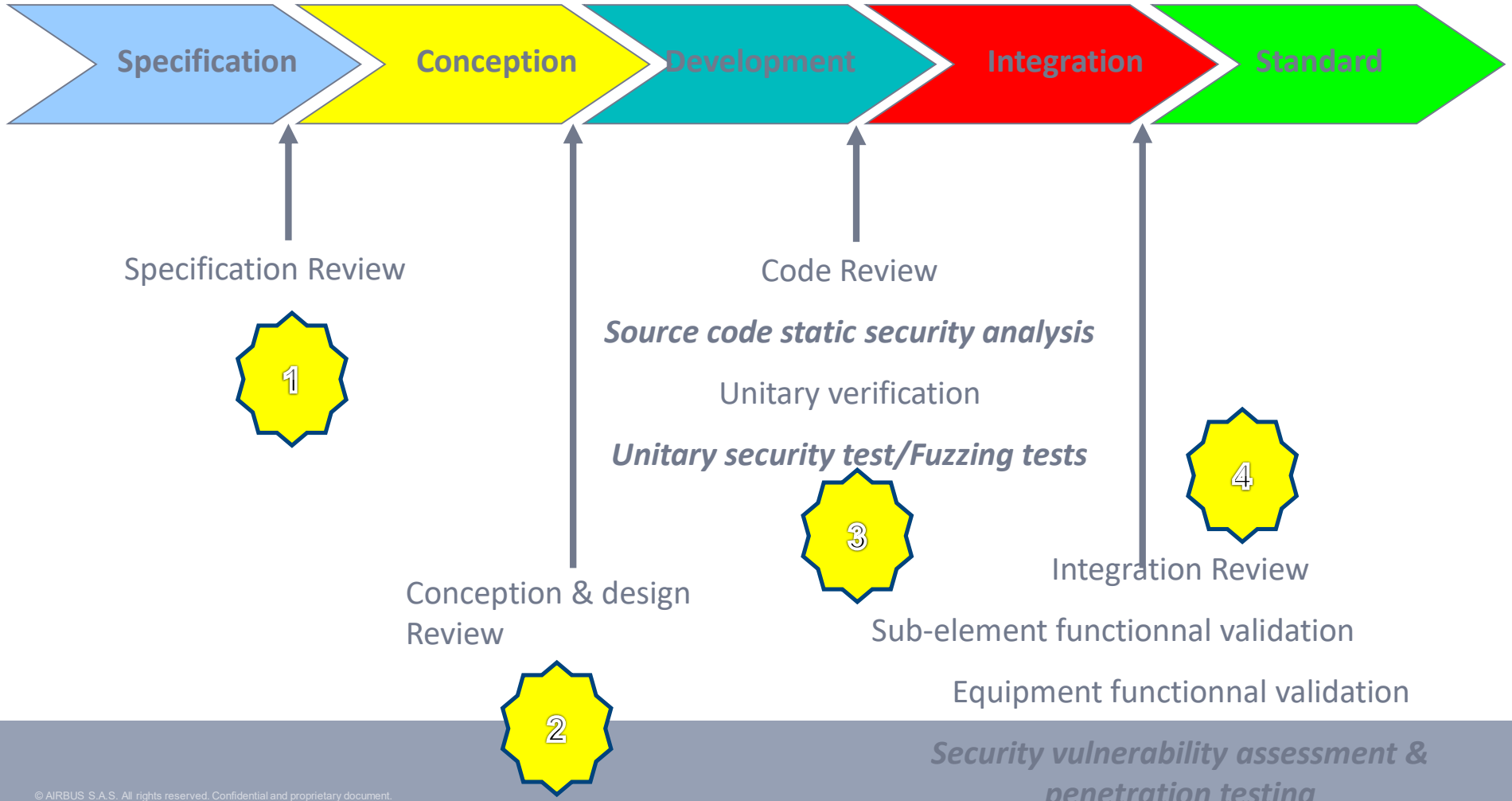
- Security activities performed at different stages:
  - ✓ Supplier Development Tests – Supplier Security Basic Testing
  - ✓ Vulnerability analysis – COTS survey/screening
  - ✓ Basic Security Tests, targeting the functional security of a system
  - ✓ Standard tests e.g. port-scanner, vulnerability-scanner, fuzzer
  - ✓ Penetration tests

Activités d'audit et d'évaluation du système d'information bord



Activités d'audit et d'évaluation du système d'information bord

Les activités d'audit securité durant les étapes dans un cycle V&V.



Activités d'audit et d'évaluation du système d'information bord

1. SPECIFICATION PHASE

- Specification review (no specific security tools required)
  - Consists in verifying the specification conformity with the requirements
  - Allows to validate that security requirements are covered
  - Shall be realized by the Software Method and Quality Team
  - Process is not different for security requirements

Activités d'audit et d'évaluation du système d'information bord

2. CONCEPTION AND DESIGN PHASE

- Conception and design review (no specific security tools required)
  - Consists in verifying the conception conformity with the specification
  - Allows to validate that security requirements are covered
  - Shall be realized by the Software Method and Quality Team
  - Process is not different for security requirements

Activités d'audit et d'évaluation du système d'information bord

3. DEVELOPMENT PHASE

- Code review
  - Consists in verifying that source code implements low level requirements
  - Allows to verify that coding norms and standard (Including security coding rules) are respected
  - Allows to validate that source code is traceable with the requirements
- Unitary verification
  - Allows to verify that object code comportment respects the requirement (including security functions)
  - Could be realized with a source code static analyzer (customized to verify the formal properties defined in conception)

Activités d'audit et d'évaluation du système d'information bord

3. DEVELOPMENT PHASE

- Source code static security analysis
  - Specific tools allow to analyze the source code
  - Aim of this tools is to find security flaws such as: null pointer, buffer overflow, memory management errors, unauthorized methods…
- Unitary Security test / Fuzzing tests
  - Allows to complete unitary functional test by testing the function in a non nominal situation
  - Consist in injecting bad entry value and analyzing the function comportment
  - Specific tools could be used

Activités d'audit et d'évaluation du système d'information bord

4. INTEGRATION PHASE

- Integration review
  - Consists in verifying that the software/Hardware is conform to the static and dynamic architecture requirements.
- Sub-Element/Equipment functional validation
  - Consist in testing the entire equipment functionality with the test plan.
- Security vulnerability tests
  - Consist in testing the equipment with a vulnerability scanner

Activités d'audit et d'évaluation du système d'information bord

4. VULNERABILITY ASSESSMENT & PENETRATION TESTING

- Vulnerability assessment
  - This is a blackbox or whitebox test that consist to scan the system with a vulnerability scanner to discover the vulnerabilities that could allow: crash the application, elevation privilege or others malicious result….
- System configuration security test
  - Consist in scanning the system configuration to valid if some configuration parameter could introduce vulnerability.

Activités d'audit et d'évaluation du système d'information bord

- En fonction du besoin, le périmètre des activités peut varier

TYPE OF TEST	DESCRIPTION
NETWORK SCANNING	A method for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer.
VULNERABILITY SCANNING	A method for identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened.
PENETRATION TESTING	A method for evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat hacker, or Cracker
PASSWORD CRACKING (BRUTEFORCE)	A method for identifying weak passwords and keys

Activités d'audit et d'évaluation du système d'information bord: Niveau Avion
Focus on USB attacks

- **Attack the host**
  - Going beyond spreading malwares
- Needing specific hardware
  - Even if very small and cheap
- Can act as **any other device**
  - Keyboard, screen, network, mass-storage…
- Software vendors dismiss USB vulnerabilities
  - As physical access is needed
- Short search on Internet
  - CVE-2011-2295: Oracle Sun Solaris USB Local Buffer Overflow Vulnerability
  - CVE-2012-3723: Apple Mac OS X USB Hub Descriptor bNbrPorts Heap overflow
  - MS13-027: The Windows 8 RNDIS kernel pool overflow
  - CVE-2013-3200: Microsoft Windows USB Descriptor Handling Local Privilege Escalation

Facedancer 10

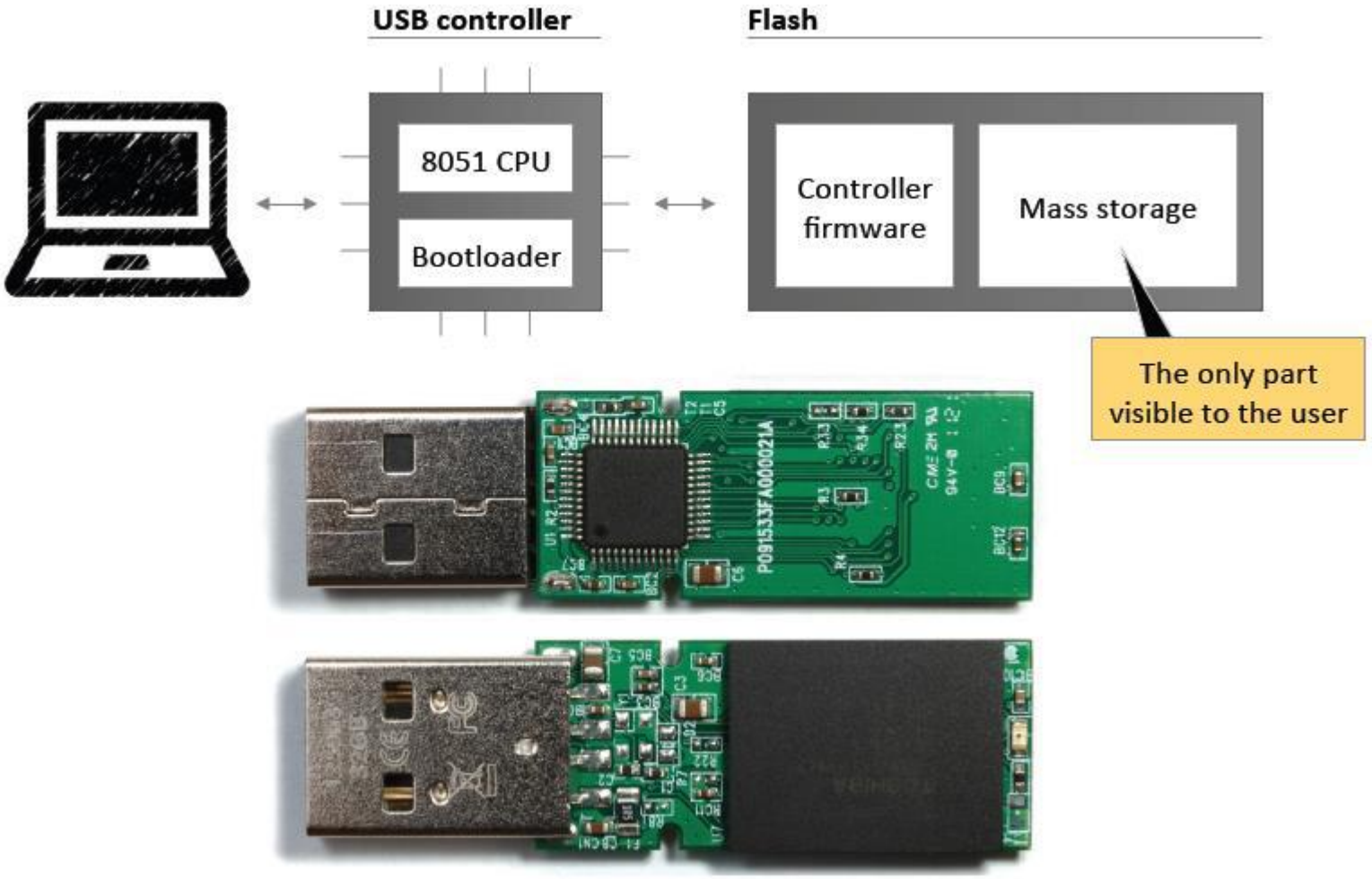

Teensy 3.0


USB Armory

USB: Universal Serial Bus
CVE: Common Vulnerabilities and Exposures

Activités d'audit et d'évaluation du système d'information bord: Niveau Avion

What is a USB stick?



Source: BadUSB – On accessories that turn evil – BlackHat USA 2014

Activités d'audit et d'évaluation du système d'information bord: Niveau système

A l'aide des même outils que pour le niveau Avion, ou avec des outils spécialisés développés pour le besoin (ex.: Scapy)

- Fuzzing,
- outils de test des interfaces USB (Teensy, Arduino, Facedancer21,…)

- Outils de test des interfaces spécifiques (ARINC A429, 1-Wire, I2C, UART, SPI, etc...)

- http://dangerousprototypes.com/docs/Bus_Pirate_v4_design_overview

Activités d'audit et d'évaluation du système d'information bord

- **SYNTHESE:**
  - Définir une stratégie/plan d'audit avec des objectifs clairs
  - Être précis sur les cas testés (enregistrements, dump, logs,..)
  - Avoir un rapport détaillé sur les vulnérabilités trouvées et leur condition d'exploitation.
  - Analyser l'impact potentiel sur le(s) asset(s) critique(s) (perte de service, perte de confidentialité ex.: DB CB) et mettre à jour les analyses de risques si nécessaire.
  - Avoir des recommandations pour corriger les vulnérabilités trouvées.
  - Assurer un suivi dans le temps
  - Définir la fréquence des futures campagnes de tests (f(criticité)).

Les centres d'évaluation

En France les CESTI agréés pour les évaluations Critères Communs et ITSEC:
http://www.ssi.gouv.fr/administration/produits-certifies/cc/les-centres-devaluation/

Types de produits logiciels et équipements réseaux

AMOSSYS	
AMOSSYS SAS, 4 bis allée du bâtiment, 35000 Rennes FRANCE	Contact : Antoine COUTANT Tél : +33 (0)2 99 23 15 79 Fax : +33 (0)2 99 23 14 27 Mél: antoine.coutant [at] amossys.fr www.amossys.fr
OPPIDA	
4-6 avenue du Vieil Etang Bât B 78180 MONTIGNY LE BRETONNEUX FRANCE	Contact : Christophe BLAD Tél : +33 (0)1 30 14 19 00 Fax : +33 (0)1 30 14 19 09 Mél : cesti [at] oppida.fr www.oppida.fr
SOGETI	**évaluation pilote en cours dans le cadre du processus d'agrément**
24, rue du Gouverneur Général Félix Eboué 92136 Issy-les-Moulineaux Cedex FRANCE	Contact : Yves Le Floch Tél : +33 (0)1 55 00 13 41 Fax : +33 (0)1 55 00 13 42 Mél : yves.le-floch [at] sogeti.com www.fr.sogeti.com

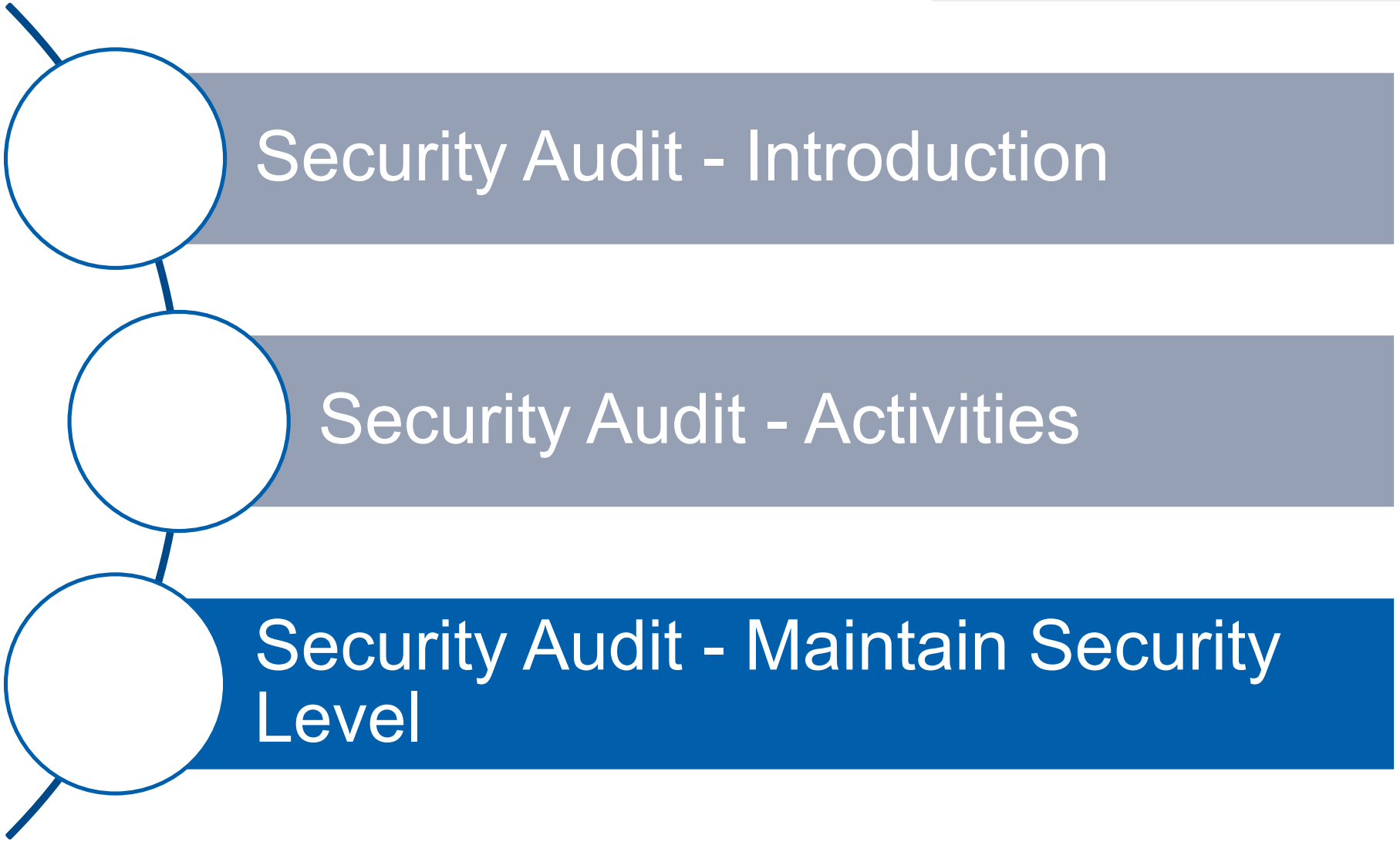
Les centres d'évaluation

- Au niveau mondial les laboratoires d'évaluation « agréés » Critères Communs: https://www.commoncriteriaportal.org/labs/

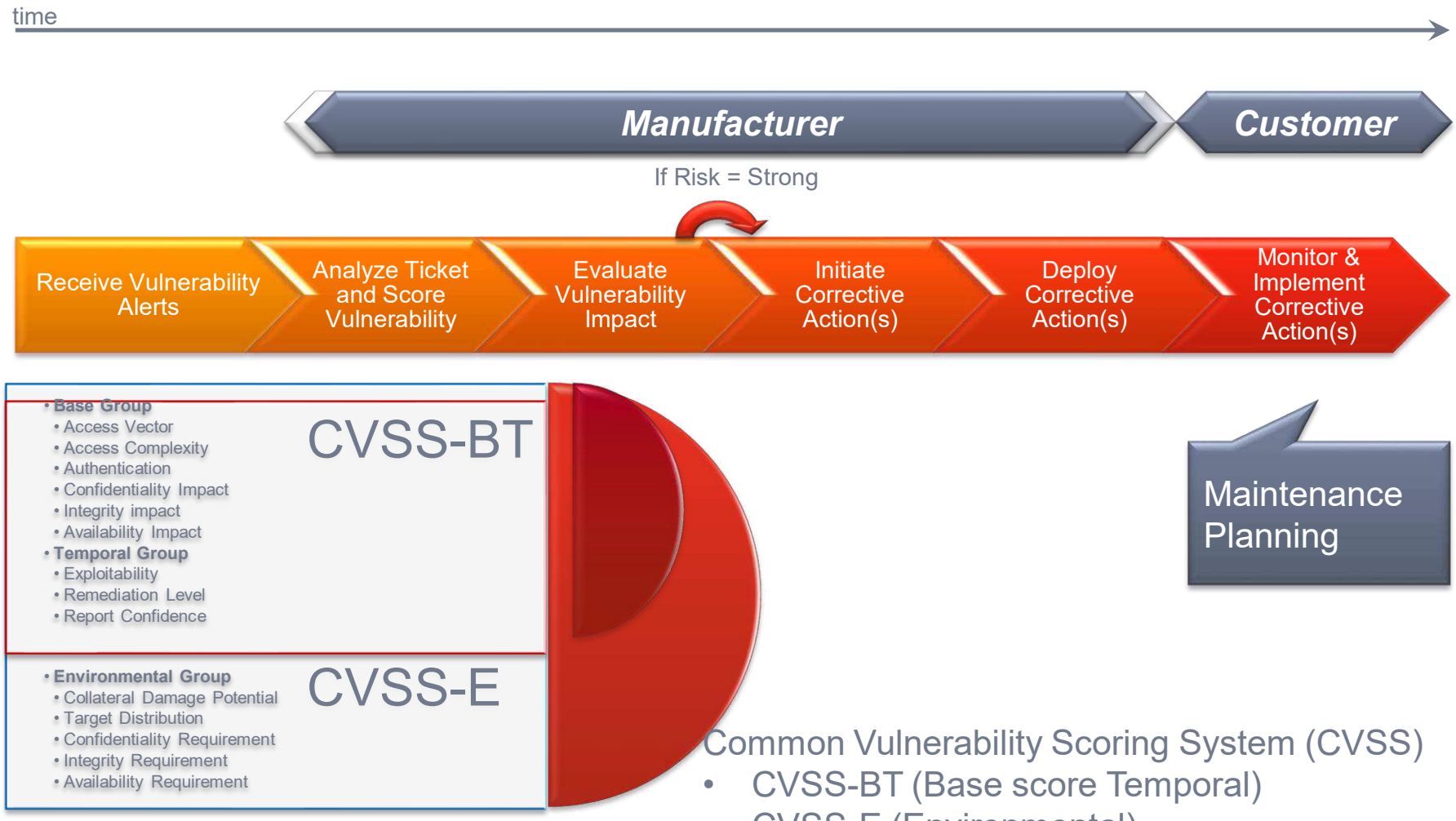
- Il existe aussi de sociétés spécialisées dans les audits/évaluation des systèmes d'information:
  - http://www.recurity-labs.com/
  - https://inversepath.com/
  - http://www.airbusgroup.com/int/en/innovation-environment/airbus-group-innovations.html

-

Summary



Gestion et suivi des vulnérabilités



Common Vulnerability Scoring System (CVSS)

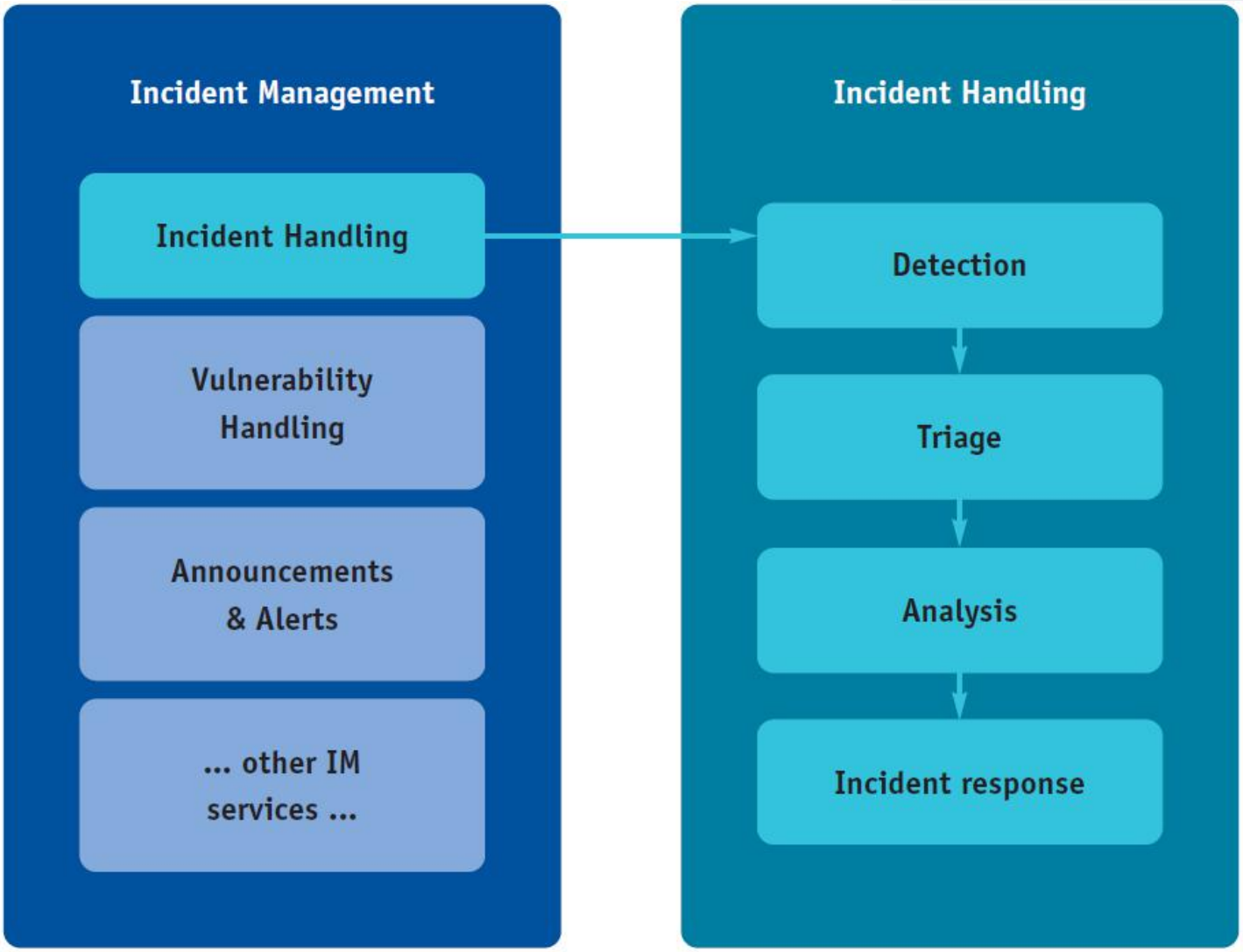
- CVSS-BT (Base score Temporal)
- CVSS-E (Environmental)

Gestion des incidents

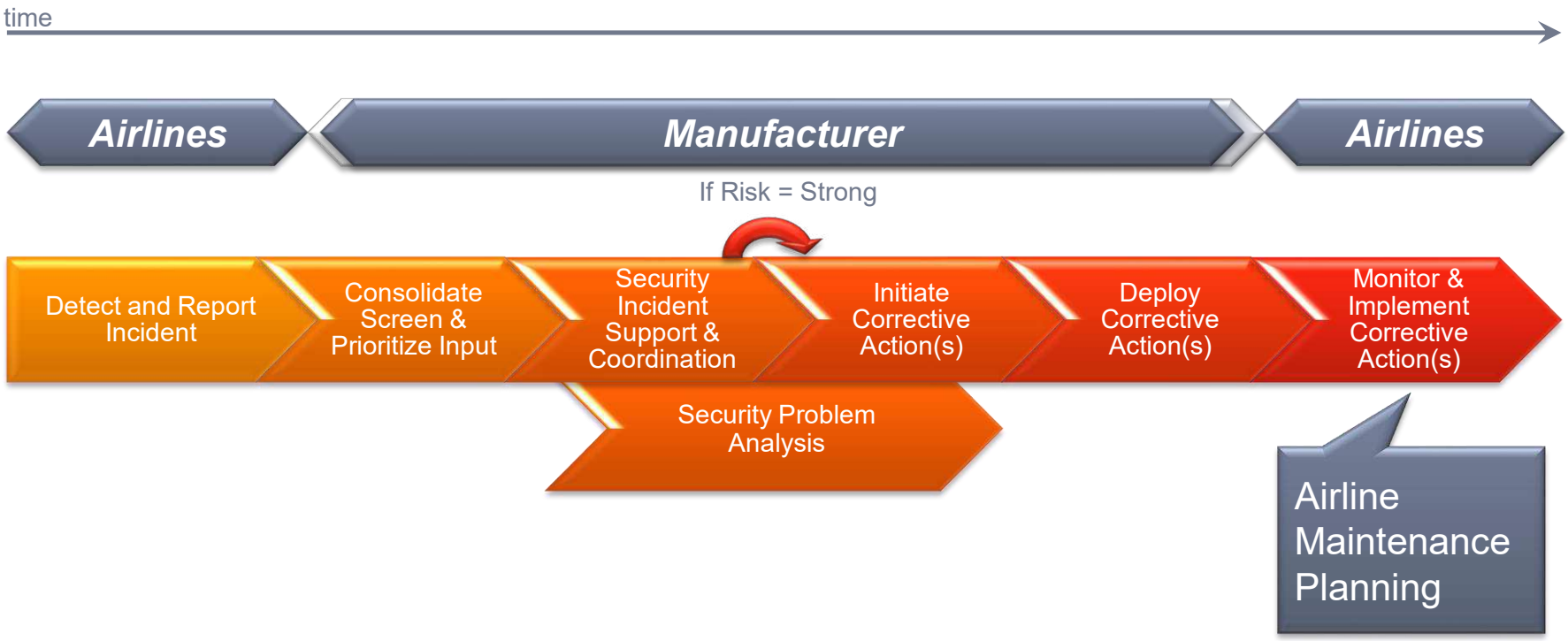
Incident Management / Handling: all defined processes, procedures, standards, documents, and individual responsibilities formalized "*to ensure a consistent and effective approach is applied to the management of information security incidents". [ISO27002:2005 - §13]*

- **Monitoring: is the action to detect unauthorized information processing** activities [ISO27002:2005 - §10.10]. This could include (but is not limited to) network monitoring (IDS/IPS), Virus scanning, logging of networks and system access and usage (ensuring accountability).
- **Security event: "an identified occurrence of a system, service or network** state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant" [ISO17799:2005]
- **Security incident: "An information security incident is made up of one or** more unwanted or unexpected Information Security events that have that could very likely compromise the security of your information or weaken or impair your business operations" [ISO27002:2005] "An event which can cause a breach of security or a loss of integrity of electronic communication networks or services" [ENISA – Technical Guideline on Reporting Incidents – Article 13a implementation]

Gestion des incidents



Gestion des incidents



Conclusion 1/2

Security is an architectural task (invent)

Security starts with Top Level Aircraft Requirements as a Multi-Systems task

Security is a full Verification-task (verify)

Top-level needs, design requirements, design verification, product verification

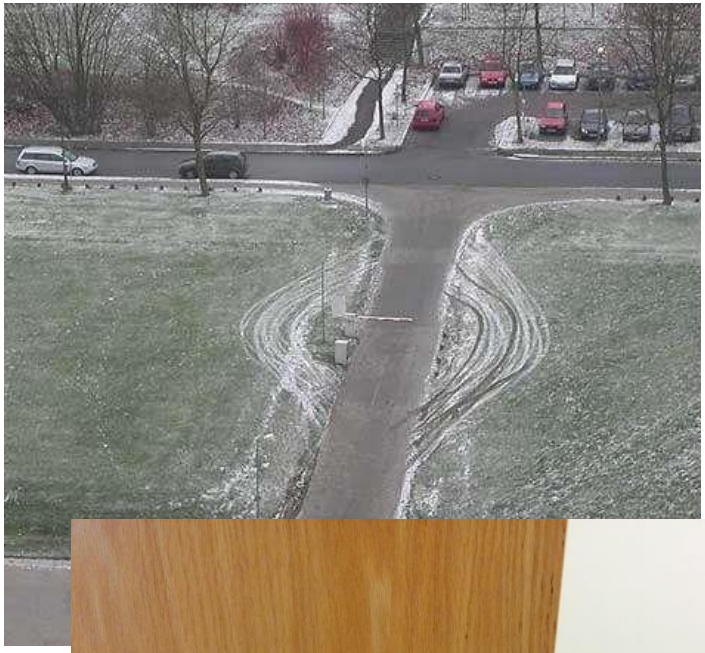
Security doesn't stop after EIS (maintain)

Vulnerability Management, Incident Management, standardization

Conclusion 2/2

- The threat is dynamic, intelligent and organized, must be monitored:
  - Do not underestimate it and take care of new/emerging threats
- Aircraft security is defined on a risk based approach
  - Priorities are driven by Risk Assessment / safety first
- Aircraft security is now fully part of V&V aircraft design processes (from inception), it has to be maintained all along its life cycle up to disposal
  - Nevertheless, the aircraft is one piece of the security chain, it cannot embed all security features.
- Coordination with / between all stakeholders (Designers, Suppliers, ANSP, AA, Airports,...) is key
  - Success relies on anticipation and joint collaboration. ALONE we are nothing

Security is a mindset



Q&A

Backup

Références

- *http://www.commoncriteriaportal.org/*
- *http://www.ssi.gouv.fr*
- *http://www.**iso**.org*
- *http://www.certa.**ssi**.gouv.fr*

Références

- Pour la conception d'une architecture sécurisée, il existe de nombreux outils sur lesquels on peut s'appuyer :
- http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html
- http://www.gns3.net/
- http://web.scalable-networks.com/content/qualnet
- …

Références

- www.ietf.org
- www.rsa.com
- www.cryptool.org
- www.insecure.org
- www.cryptographyworld.com
- S-t-d.org
- www.securiteinfo.com
- www.sha1.fr
- www.md5.fr

Références

- http://www.cert.org
- http://www.enisa.europa.eu/cert_inventory/
- http://cert.surfnet.nl/
- http://www.first.org/cvss
- http://www.isecom.org/research/
- http://en.wikipedia.org/wiki/Vulnerability_assessment
- http://secunia.com/vulnerability_intelligence/
- http://www.sans.org/reading_room/whitepapers/threats/implementing-vulnerability-management-process_34180

PRÉSENTATION DU MÉTIER D'INTÉGRATEUR

Intégration de réseaux et systèmes sécurisés pour l'aviation civile

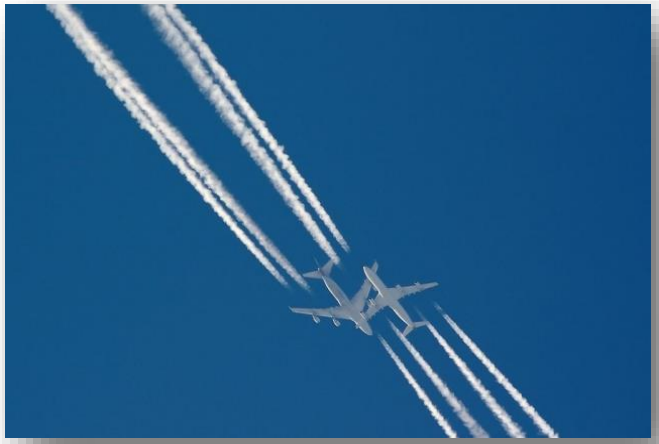
Aurélien Bouzon

Ingénieur sécurité réseaux et systèmes

TLS-SEC

08/01/2019

Plan



I. PRÉSENTATION

1. La société de service

Société de Service en Ingénierie Informatique (**SSII**)

↓

Entreprise de Services du Numérique (**ESN**)

Gammes de service :

- ➔ Conseil / Assistance
- ➔ Intégration
- ➔ Infogérance

Offre une forte diversité de missions ce qui permet d'appréhender beaucoup de milieux / technologies en « peu » de temps

Beaucoup, beaucoup de concurrence :

Capgemini, Atos, IBM, Accenture, Steria, OBS, CGI, GFI, Econocom …

Les certifications

un business, une reconnaissance par les entreprises

Certifications sécurité de consultants Atos	Nombre
CISSP	129
CISA	31
CISM	24
Certified Ethical Hacker CEH	21
ISO 27001 Lead Auditor	48
BSI IT Grundschutz	6
PCI DSS QSA	6
Other Security related certifications	355
Total	**620**

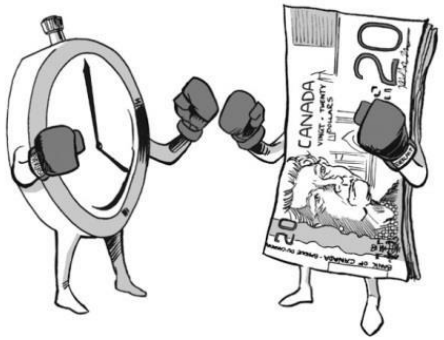
I. Présentation
2. Le métier d'intégrateur
Le travail d'un intégrateur

- **AMO(A)** : Assistance à Maitrise d'Ouvrage
  → conseil, accompagnement, expertise technique
  → pilotage, gestion de projet

- **Intégrateur** : sélectionner et assembler des briques système (software ou hardware) pour répondre à un besoin client.

1. Découverte de l'environnement client
2. Recueil du besoin client (contexte client)
3. Proposition de solutions (coût / complexité)
4. Développement / intégration
5. Test / validation
6. Déploiement
7. Support

- Un projet doit être réalisé dans les temps
  → importance du chiffrage des activités
  → pas de retard pour éviter l'insatisfaction client
  → pas de retard pour ne pas perdre d'argent



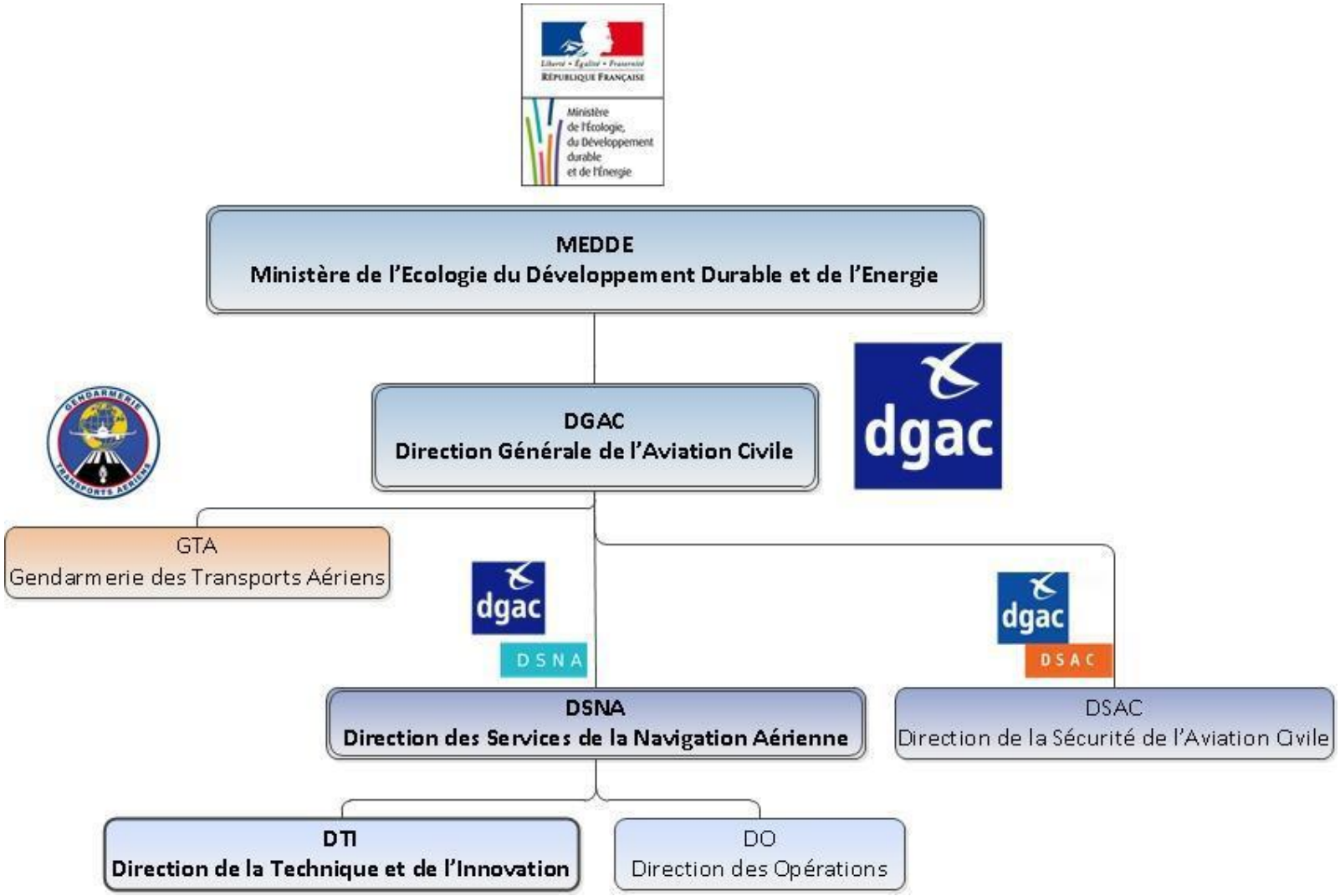
I. Présentation
2. Le métier d'intégrateur
Les livrables

- **Des livrables à produire :**
  - Cahier des charges / Exigences
  - Etudes préliminaires de faisabilité
  - Comparatif et test de produits / Etude comparative
  - Etude d'architecture / Etude d'évolution
  - Revues client
  - Dossier d'architecture / Dossier de conception
  - Dossier de tests / Dossier de validation / Dossier de recette usine
  - Manuels d'utilisation / Manuels d'installation
  - Documents liés à la conduite de projets (compte rendu de réunion, recadrage du projet …)
  - Eventuellement un produit logiciel ou matériel
  - Gérer les phases de migrations
  - … et bien d'autres

→ Souvent beaucoup de documentation

→ La documentation annexe est en général aussi conséquente, sinon plus, que le produit fini lui même

I. Présentation
3. Aviation Civile
Organigramme



I. Présentation
3. Aviation Civile
La DSNA

dgac

DSNA

Prestataire de service de la Navigation Aérienne

- Fournit les services permettant le bon déroulement de l'activité de contrôle aérien.

- Echanges avec :
  - des partenaires Européens
  - des partenaires mondiaux (DOM/TOM)
  - des partenaires industriels
  - des compagnies aériennes
  - des gestionnaires d'aéroport
  - Météo France
  - L'armée
  - Les usagers
  - …

EUROCONTROL

Aena Aeropuertos Españoles y Navegación Aérea

Belgocontrol

DFS Deutsche Flugsicherung

skyguide

ENAIRE

NAV CANADA

FEDERAL AVIATION ADMINISTRATION

AÉROPORTS DE PARIS

AIRFRANCE

AÉROPORTS de LYON

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

METEO FRANCE

I. Présentation
3. Aviation Civile
La DTI

- Missions : définir, faire réaliser et installer les systèmes techniques utiles au contrôle Aérien.

Radar :
- Primaire : pulse / echo
- Secondaire : transpondeur
- Air
- Sol
- Multilatération

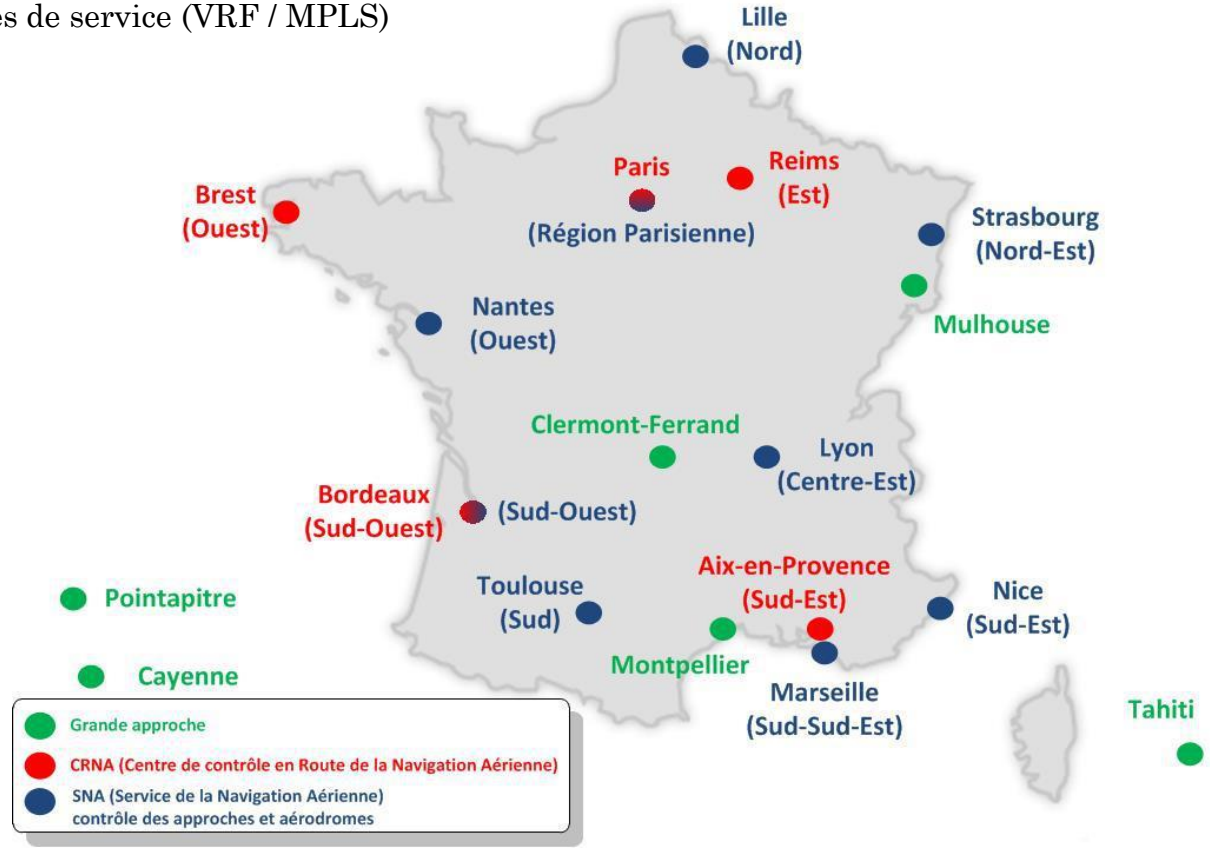
Assistance au contrôle
- écran RADAR
- Strips
- messagerie aéronautique
- Téléphonie
- DMAN (Départure Manager)
- AMAN (Arrival Manager)

Assistance au pilotage
- Radio
- VOR
- DME
- ILS

Réseau
- WAN
- LAN
- Supervision
- Sécurité

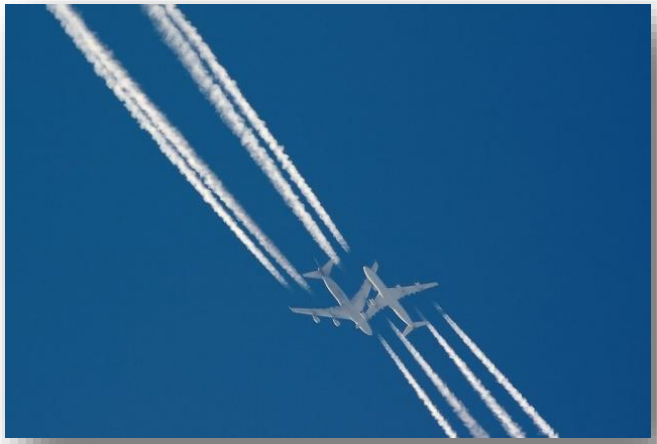
I. Présentation
3. Aviation Civile
Un Réseau national : RENAR IP

- Réseau national, remplaçant le réseau RENAR (X25), qui véhicule les données du transport aérien
- Eviter les points de défaillance unique (SPoF : Single Point of Failure)
  - Réseau maillé
  - S'appuie sur plusieurs opérateurs et arrivées (indépendance des arrivées et des chemins)
  - Exploitation d'une longueur d'onde (lambda)
  - Classes de service (VRF / MPLS)



Plan

I. Présentation
II. **Contexte / Enjeux**
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion



II. Contexte / Enjeux
Pourquoi de la sécurité pour la DSNA ?

L'aviation civile passe d'un monde fermé à un monde de plus en plus "ouvert"

Informations sur le trafic aérien (accessibles pas construction)

- Radio
- Horaires des vols / quasi temps réel (tableau d'affichage aéroport)

Sur Internet (partage de l'information)

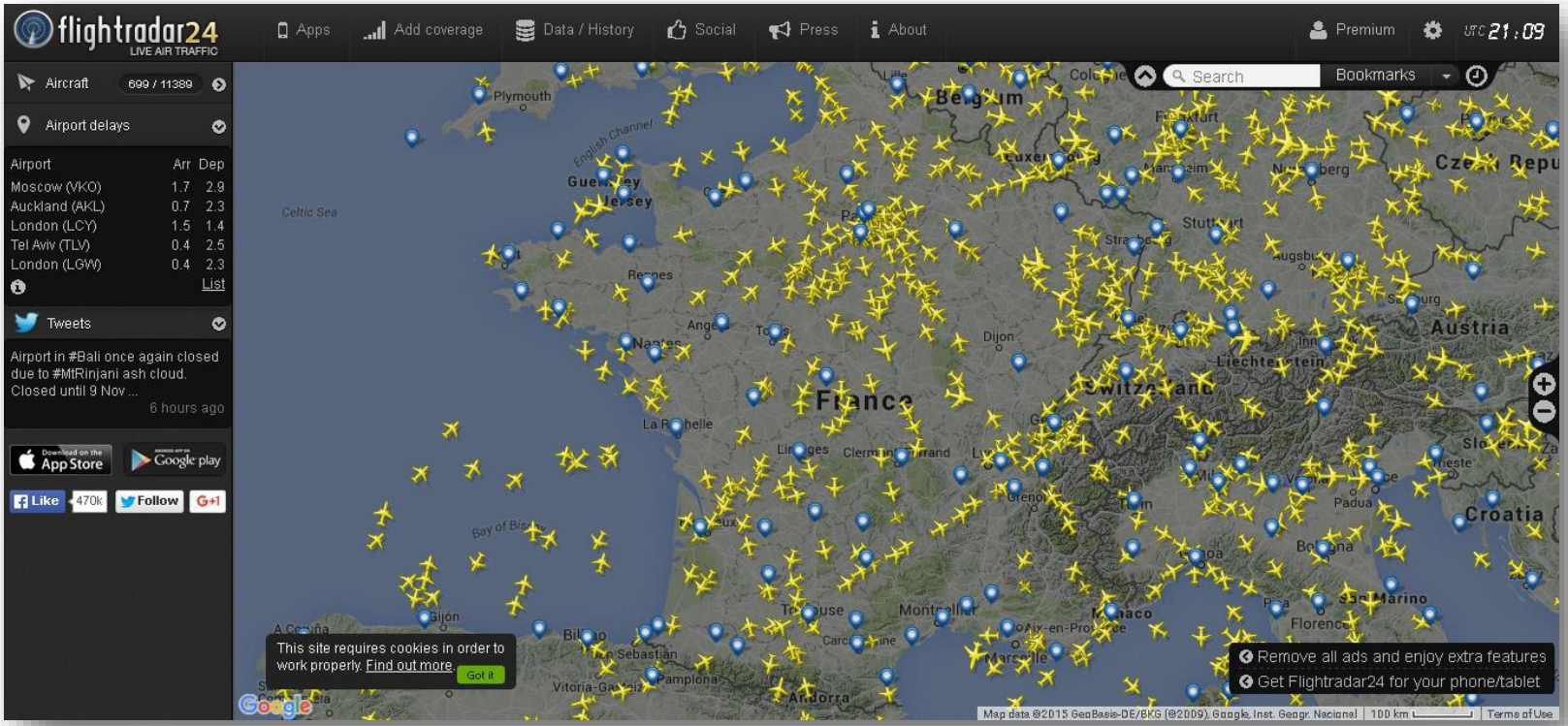
- **ADS-B**
- **Dépose de plan de vol / Actualité aéroportuaire**

Dans l'avion (toujours plus connecté)

- Internet en vol par satellite et station de base au sol
- Wifi (divertissement et information d'exploitation)
- Ecran de divertissement dans l'avion (souvent un linux intégré)

II. Contexte / Enjeux
ADS-B

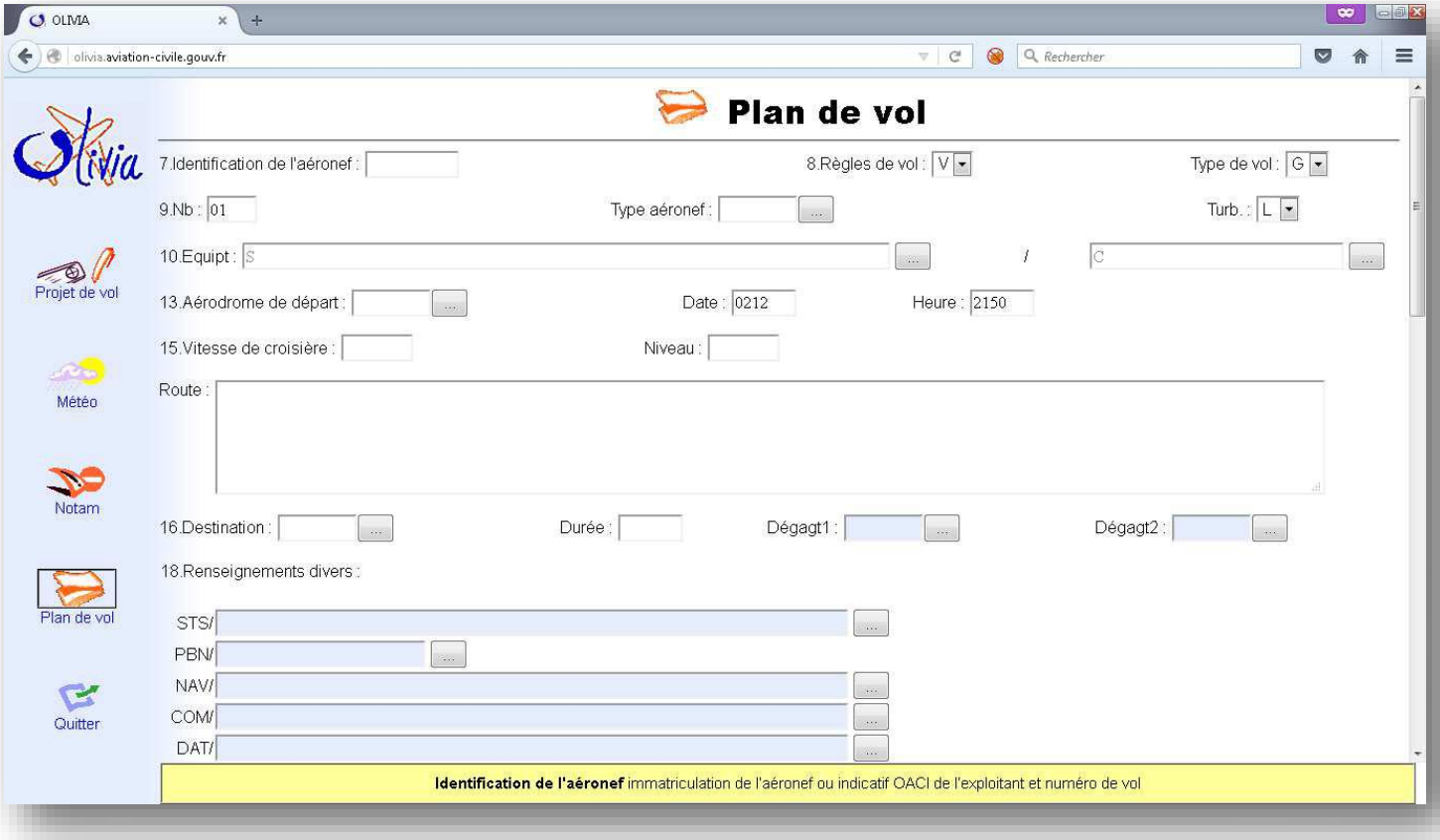
- Diffusion de l'information par l'avion (position, vitesse, direction)
  - Corruption possible → créer un avion en diffusant des informations
  - Information très précise (trop ?)
  - Système conçu avant tout pour être fonctionnel, la sécurité n'était pas une priorité lors de la conception



II. Contexte / Enjeux
Plan de Vol

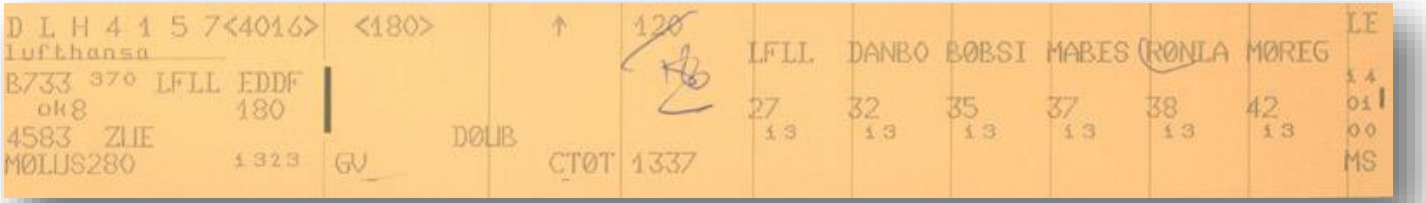
- Dépose libre sur Internet
- Notam (Notice to Airmen) : informations aux navigants

➔ Service en ligne Olivia (http://olivia.aviation-civile.gouv.fr/)



II. Contexte / Enjeux
Gestion électronique

- Avant, tout était géré sous forme papier (plan de vol, stripping, parking)



- Aujourd'hui le stripping est le dernier élément à se dématérialiser

- Système ERATO (En Route Air Trafic Organizer)
  - Optimisation du trafic
  - Couplage à d'autres systèmes pour : économie de kérosène / réduction des retards (DMAN/AMAN)
  - Existence virtuelle de l'avion (plus de strip papier)
  - Des contraintes :
    - Double source électrique
    - Redondance du matériel
    - Duplication de la donnée

- Convergence vers un ciel unique → projet 4Flight

II. Contexte / Enjeux
Quel type de sécurité ?

Confidentialité

- L'aviation civile n'a rien à cacher
- L'information est en très grande partie disponible librement

Authenticité

- **Données radio**
  - Pensée en premier lieu pour la fiabilité de fonctionnement
  - Garantie par le moyen de communication (fréquence radio nécessite une licence)
  - Aucune garantie réelle → protégé par la lourdeur de la sanction
- **Données réseau**
  - Fortes garanties (VPN, liaisons spécialisée)

Intégrité → ce qu'il faut garantir en priorité

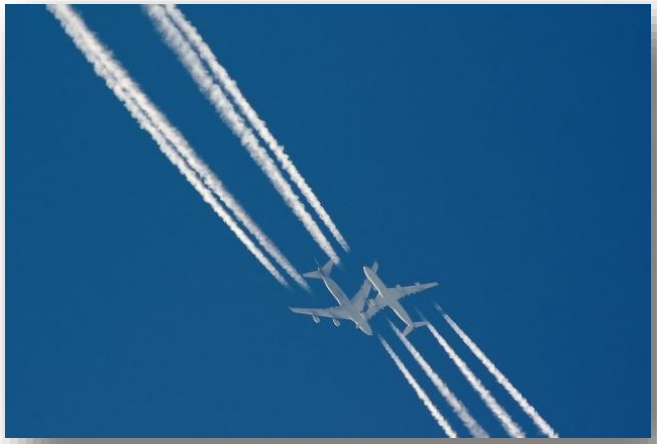
- **Données radio** : code OTAN, phraséologie
- **Données réseau** : Réseau propriétaire (engagement contractuel)

Non-répudiation

- Enregistrements légaux (flux radar, plan de vol, radio)

Plan

I. Présentation
II. Contexte / Enjeux
III. **Aspects réglementaires**
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion



III. Aspects réglementaires
Statu d'OIV (Opérateur d'Importance Vitale)

D'après le Code de la Défense :

- « gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont **le dommage ou l'indisponibilité ou la destruction** par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement **d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation** ;

- ou de mettre gravement en cause la santé ou la vie de la population ».

III. Aspects Réglementaires
Des textes

LPM : Loi de Programmation Militaire

- Les obligations des OIV
  - Notifier l'ANSSI en cas d'incident de sécurité
  - Les modalités de validation / audit (ANSSI)
  - Isoler certains systèmes d'Internet
  - Surveiller son réseau
- Les sanctions en cas de non respect des obligations

ESARR : European Safety Regulatory Requirements

- Harmonisation et l'amélioration de la sécurité au niveau Européen
- Rédigé par Eurocontrol

PSSI : Politique de Sécurité des Système d'Information

- Organisation autour du SI
- Les acteurs
- Les domaines / réseaux / zones et leur rôle (à très haut niveau)
- Les règles d'échange (matrice de flux)
- Les principes généraux spécifiques au métier (focaliser la protection sur ce qui a le plus d'importance)

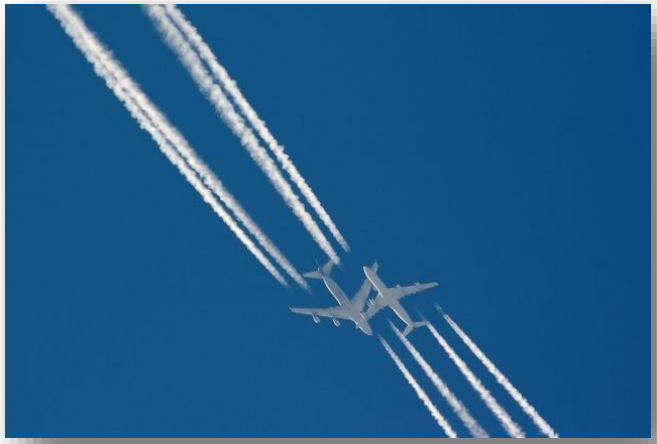
III. Aspects réglementaires
ANSSI : Agence National de la Sécurité des Systèmes d'Information

Les rôles de l'ANSSI

- Conseil / assistance pour les intérêts français :
  - *OIV*
  - *grandes entreprises Françaises*
  - *PME*
- Surveillance / audit (OIV)
- Qualification de matériel (qualifié standard)

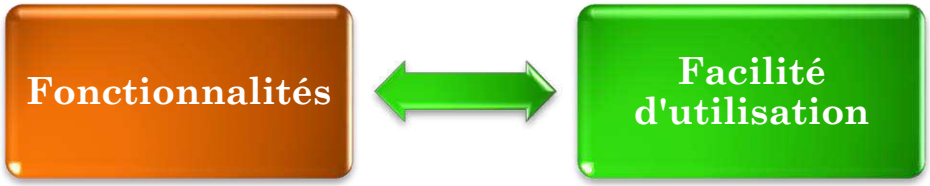
Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. **Architecture réseau**
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion



IV. Architecture réseau
Trouver le bon compromis

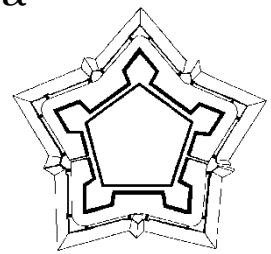
- Bien / vite réagir en cas d'incident → besoin de simplicité
- Besoin de fonctionnalités et d'ergonomie
- Toujours plus de sécurité



IV. Architecture réseau
Définition

Architecture sécurisée

- Manière de structurer le SI pour qu'il soit le plus adapté à l'organisation et au besoin métier
- Repose sur la manière de cloisonner et d'interconnecter
  - Réseaux cloisonnés (segmentation)
  - Réseaux à plat (simple, propagation facilitée)
- Hérite des connaissances militaires (châteaux forts, fortifications de Vauban, prisons, structures panoptiques)



Doit répondre à des problématiques de base :

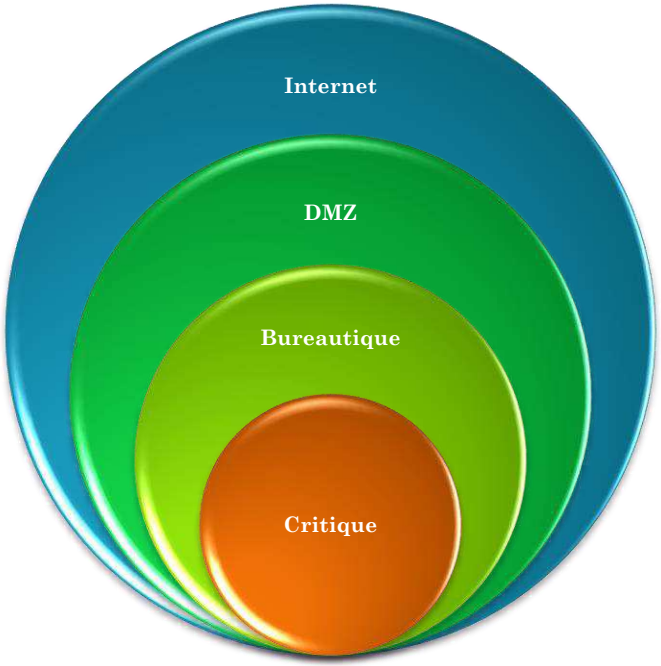
- Débits
- Technologies
- Disponibilité

IV. Architecture réseau
Sécurité périmétrique

Sécurité périmétrique :

- Modèle de protection concentrique
- Chaque niveau de protection est délimité par un élément filtrant (pare-feu)
- Si le périmètre est cassé à un endroit, tout le niveau est corrompu
  - → c'est le maillon le plus faible qui détermine le niveau de sécurité

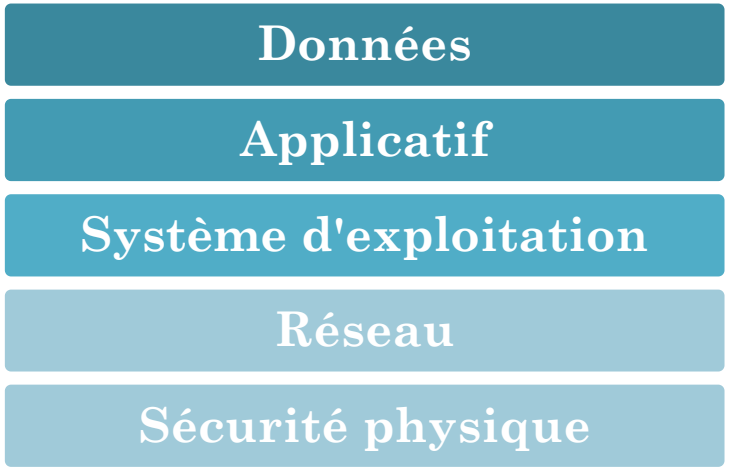
- Le moins critique à l'extérieur
- Le plus critique au centre



IV. Architecture réseau
Défense en profondeur

Sécurité / défense en profondeur

- Sécurisation de toutes les couches OSI "du physique à la donnée"
- Augmente la probabilité de détection d'une attaque
- Diminue les impacts et la vitesse de progression d'une attaque



➔ Actuellement on trouve, le plus souvent, une combinaison des deux approches (périmétrique et en profondeur)

IV. Architecture réseau
La sécurité physique

La sécurité physique poussée à l'extrême

- Isoler le système / réseau de toute interconnexion
- Le placer dans un endroit très protégé (barbelés, bunker, chiens …)

- → Le système / réseau est tellement bien protégé qu'il est inaccessible / inutilisable

- → **La sécurité d'un SI n'est rien sans sécurité physique**
- il est toujours possible de reprendre le contrôle d'un équipement (reset usine)
- → Nécessité du contrôle d'accès

- Favoriser la double authentification
  - Ce que je sais (code)
  - Ce que je suis (biométrie)
  - Ce que je possède (badge)

IV. Architecture réseau
L'ingénierie sociale

Des moyens de "se protéger" de l'humain :

- **Cacher l'information / sécurité par l'obscurantisme** (architecture, type de matériel, procédures …)
- → Permet de **se protéger d'un attaquant extérieur**

- **Formation / sensibilisation contre l'ingénierie sociale**
- → l'ingénierie sociale permet d'obtenir l'information cachée ou un accès
- Pour récupérer l'information **un attaquant externe s'expose / se fait connaître**
- Cacher l'information garde donc un intérêt mais ne peut pas être la seule mesure de protection

- **Habilitation** / surveillance du personnel
- → Permet de **se protéger d'un attaquant interne**

- **Organisation** / segmentation du travail et des connaissances
- → Permet de **se protéger d'un attaquant interne et externe**

IV. Architecture réseau
Les principes de base

Protéger ce qui a le plus de valeur

- Identifier la valeur ajoutée à protéger

Tout ce qui n'est pas autorisé est interdit

Pas d'adjacence de réseau / Pas de double raccordement

- Eviter de raccorder deux zones de criticité différente à un équipement non filtrant → casse la segmentation

Isoler les fonctions / Dédier des systèmes

- A modérer avec l'aspect budgétaire

Maximiser la segmentation / Eviter les réseaux à plat

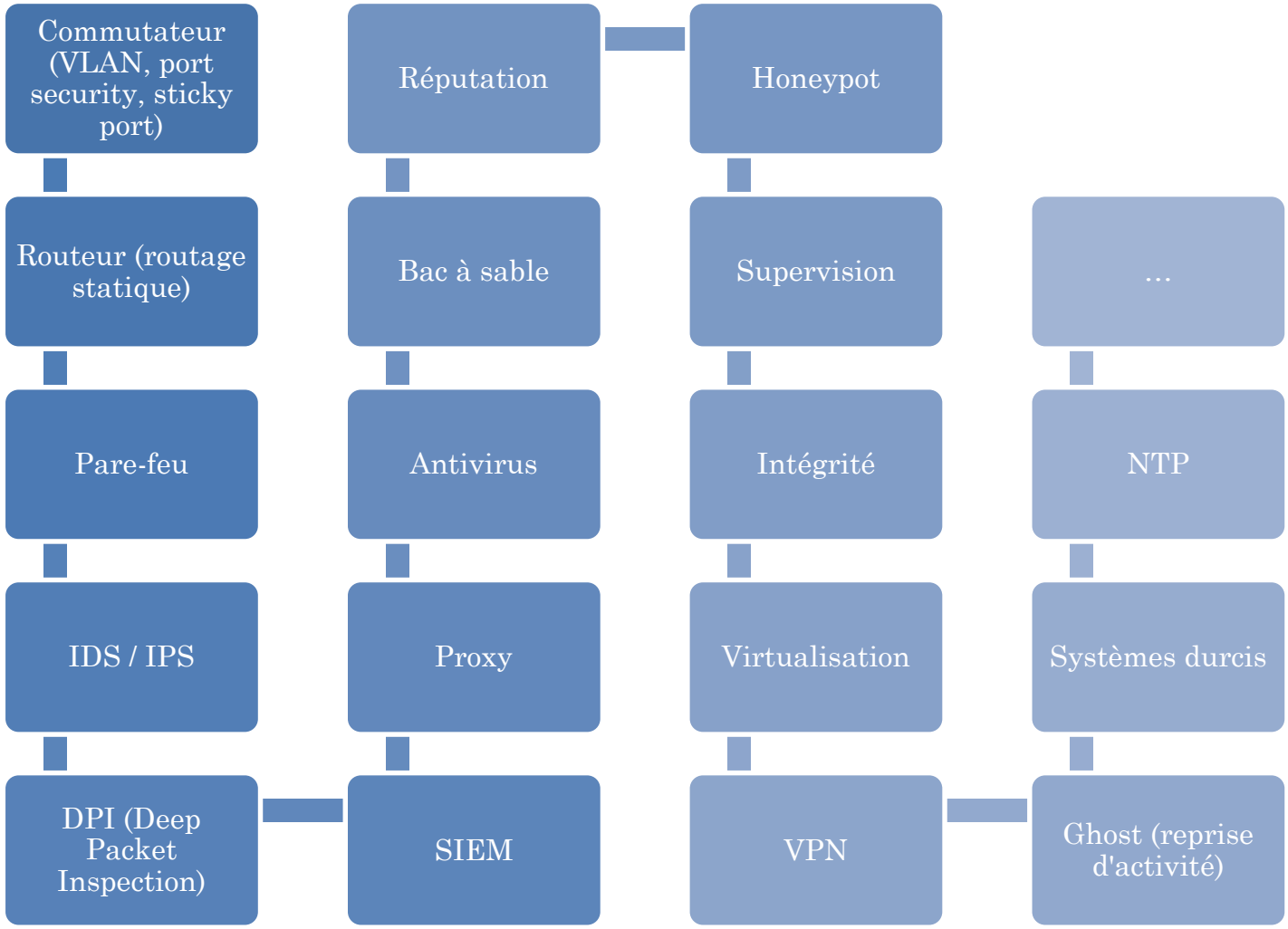
- Compromis : complexité / coût / intérêt
- Permet d'identifier plus facilement les flux (source / destination)

Maximiser les performances de l'architecture

Eviter les points de défaillance unique / Offrir de la disponibilité

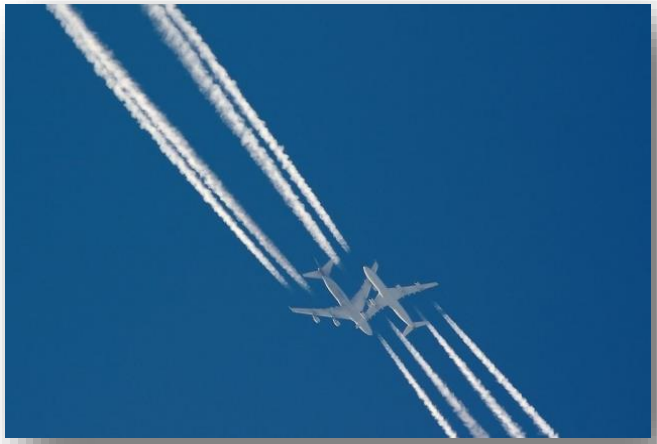
- Compromis : besoin / coût
- SPoF : Single Point of Failure
- Mutualiser/ rationaliser

IV. Architecture réseau
Les outils techniques



Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. **Cas d'application**
    1. **Architecture de base**
    2. **Filtrage applicatif**
    3. **Réplication**
    4. **Disponibilité**
    5. **DoS**
    6. **Détection d'intrusion**
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion



V. Cas d'application
1. Architecture de base
Besoins

Besoins :

- Permettre la dépose des plans de vol depuis Internet
- Récupérer / envoyer des plans de vol de partenaires
- Solution économique

- Segmentation du réseau
- Limiter l'exposition du serveur (services)
- Ne pas donner l'accès au réseau partenaire depuis Internet
- Se protéger de ce qui pourrait venir du partenaire
- Ouvrir les flux à partir d'une matrice de flux identifiée
- Mise en place de règles de filtrage sur un pare-feu
- Masquer l'adresse réelle du serveur (NAT Network Adress Translation) au niveau du pare-feu

V. Cas d'application

1. Architecture de base

Matrice de flux

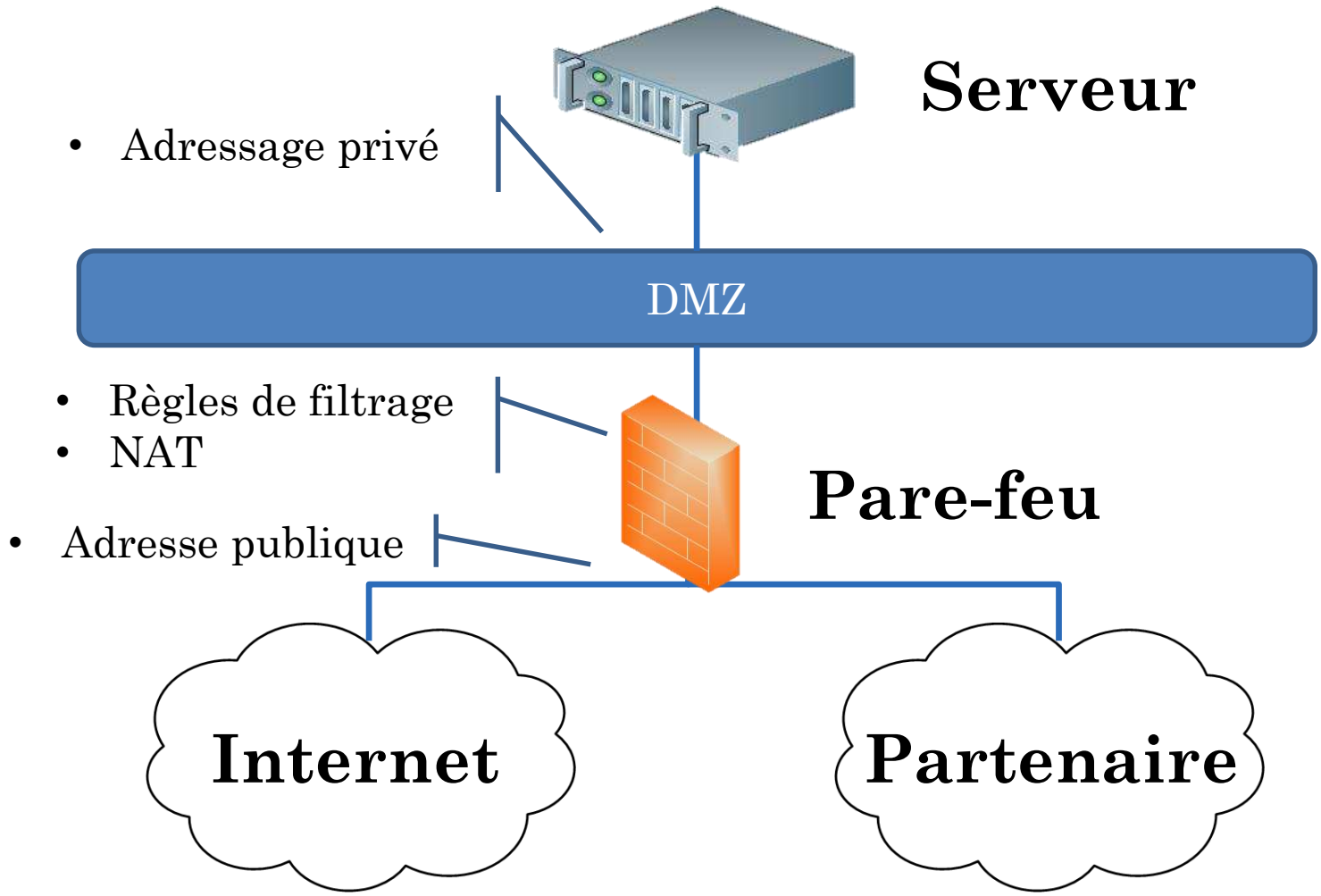
- Le sens d'initialisation d'une connexion importe (TCP SYN ou pseudo connexion UDP)
- La règle dans le sens retour est implicite avec un pare-feu à état (statefull)

Source / destination	Internet	Partenaire	DMZ
Internet			
Partenaire			✓
DMZ	✓	✓	

V. Cas d'application

1. Architecture de base

Schéma



V. Cas d'application
1. Architecture de base
Pare-feu

- Elément de base pour le filtrage entre les réseaux
- Fait une grande partie du travail
  - Règle de filtrage (ACL) niveau 3 et 4
  - NAT
  - Routage
- Existe maintenant sous forme d'appliance virtuelle
- Les appliances physiques ont de meilleures performances ASIC (Application Specific Integrated Circuit)
- Relativement peu d'interfaces (GigaEthernet, Fibre), n'est pas fait pour collecter
- Débit de filtrage limité (quelques giga pour du milieu de gamme)
- Débit souvent limité par les fonctionnalités tierces (antivirus, IPS …)

- Les fabricants proposent aujourd'hui des UTM/USM (Unified Threat/Security Management)
  - IDS/IPS
  - Antispam
  - Antivirus
  - Proxy HTTP
  - Proxy SSL
- Pratique mais va contre le principe de séparation des fonctions (SPoF)

1. Architecture de base

Pas de pub, une vision du marché du pare-feu

V. Cas d'application
2. Filtrage applicatif
Besoins

Besoins :

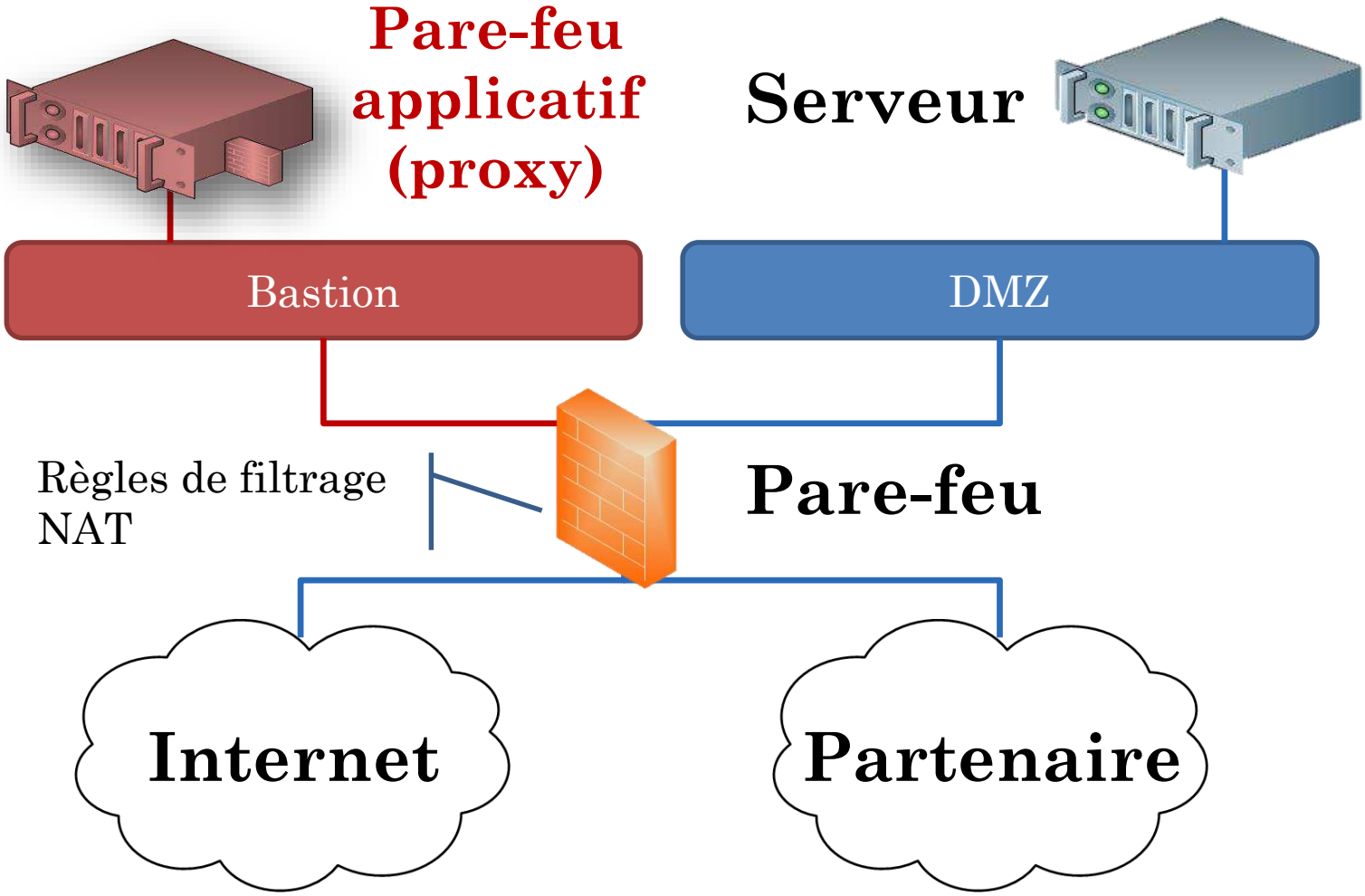
- N'autoriser que les requêtes bien formées

- Réaliser un filtrage de niveau applicatif
- Dédier une machine à ce traitement (proxy)
- Positionner le proxy dans une zone distincte (bastion)

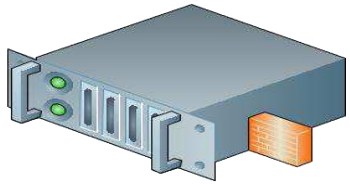
Source / destination	Internet	Partenaire	Bastion	DMZ
Internet				
Partenaire			✓	
Bastion	✓	✓		✓
DMZ			✓	

2. Filtrage applicatif

Schéma



V. Cas d'application
2. Filtrage applicatif
Proxy



Pare-feu de niveau 7 (applicatif)

- Inspecte / filtre la donnée de niveau applicatif
- Réalise une rupture dans la connexion

WAF (Web Application Firewall) = proxy web

- Filtrage URL
- Filtrage paramètres (taille, type, valeur)
- …

Les REGEX sont très utilisées :

- Whitelist/blacklist URL (Pare-feu/Proxy)
- Filtrage de paramètres
- Mais aussi : règle de corrélation (SIEM), Parser (SIEM), IDS, scripting …

Le monde ne se limite pas au web !

- Proxy : SNMP, SYSLOG, NTP, FTP …
- Quid proxy pour protocole non standard / répandu ?
- → Nécessite un développement spécifique

V. Cas d'application
3. Réplication
Besoins

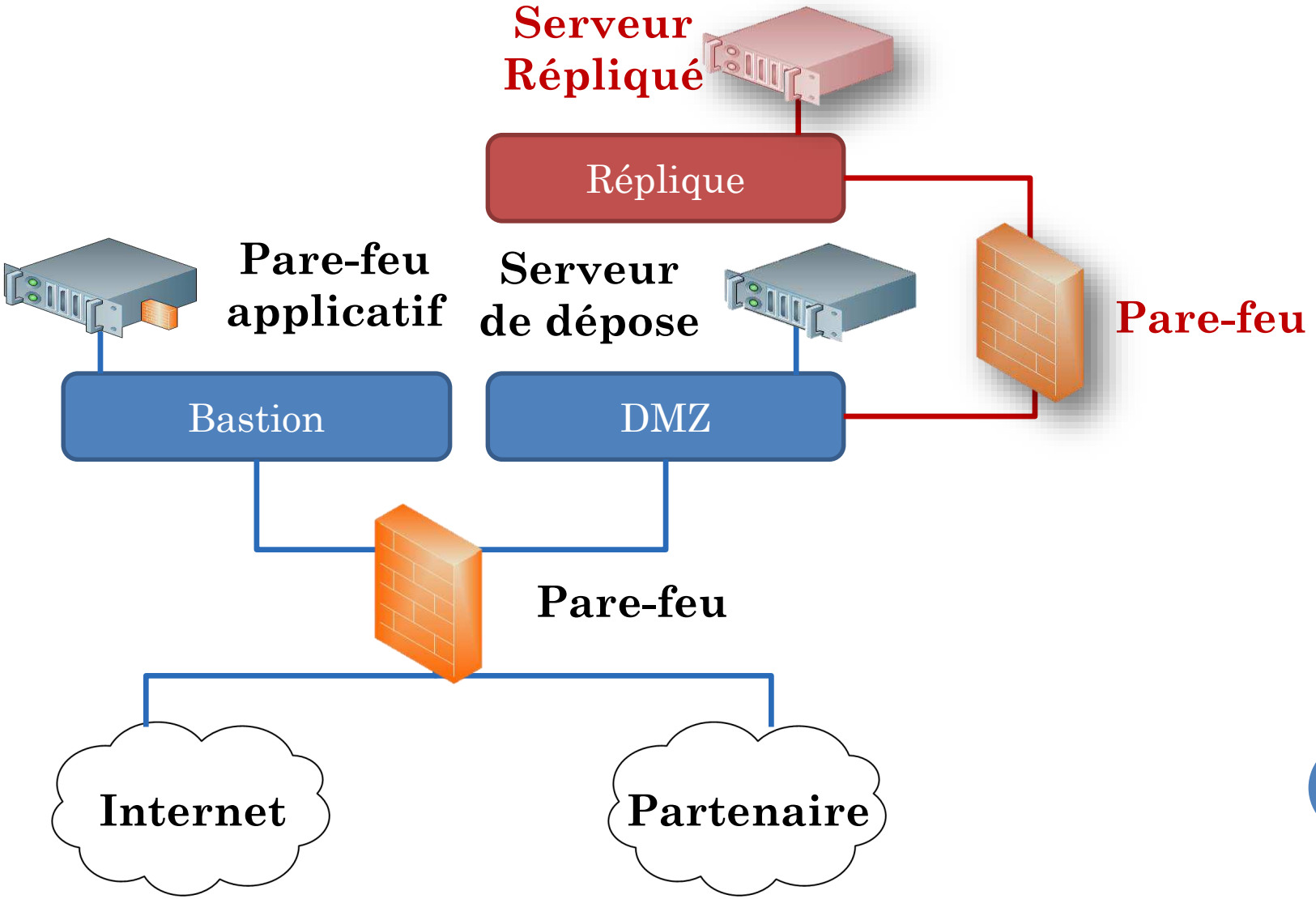
Besoins :

- Empêcher la compromission des plans de vol utilisés pour le contrôle
- Permettre la modération des plans de vol déposés

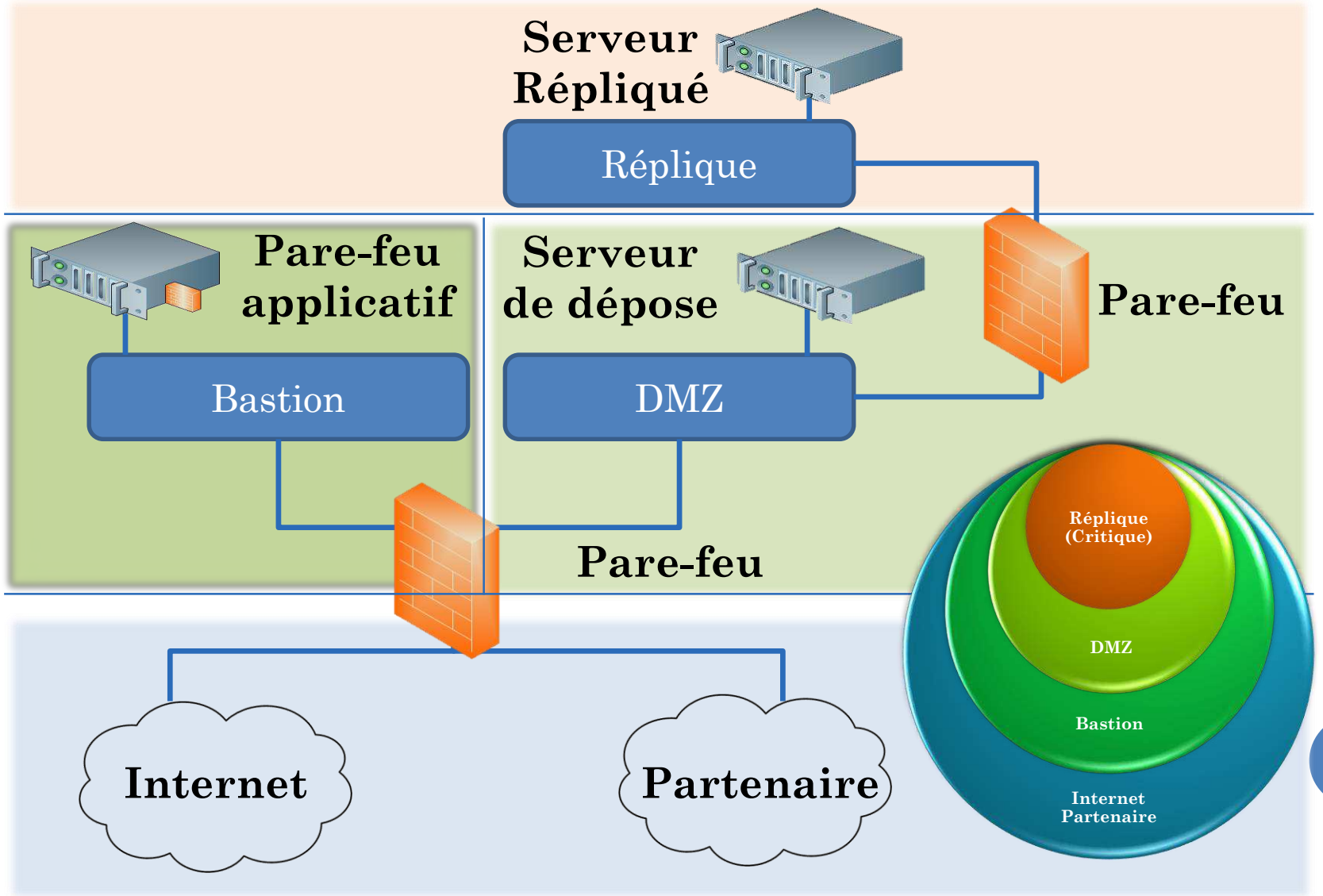
- Mise en place d'un serveur de plan de vol répliqué
- Création d'une zone spécifique pour le serveur répliqué (réplique)

Source / destination	Internet	Partenaire	Bastion	DMZ	Réplique
Internet					
Partenaire			✓		
Bastion	✓	✓		✓	
DMZ			✓		✓
Réplique					

V. Cas d'application
3. Réplication
Schéma



V. Cas d'application
3. Réplication
Schéma - zones



V. Cas d'application
4. Disponibilité
Besoins

Besoins :

- Offrir plus de disponibilité
- Optimiser la réponse à la charge vs consommation énergétique
- Accélérer la reprise d'activité
- Faciliter la maintenance
- Faciliter la mise en place d'évolutions

- Double source électrique (groupe électrogène, batterie)

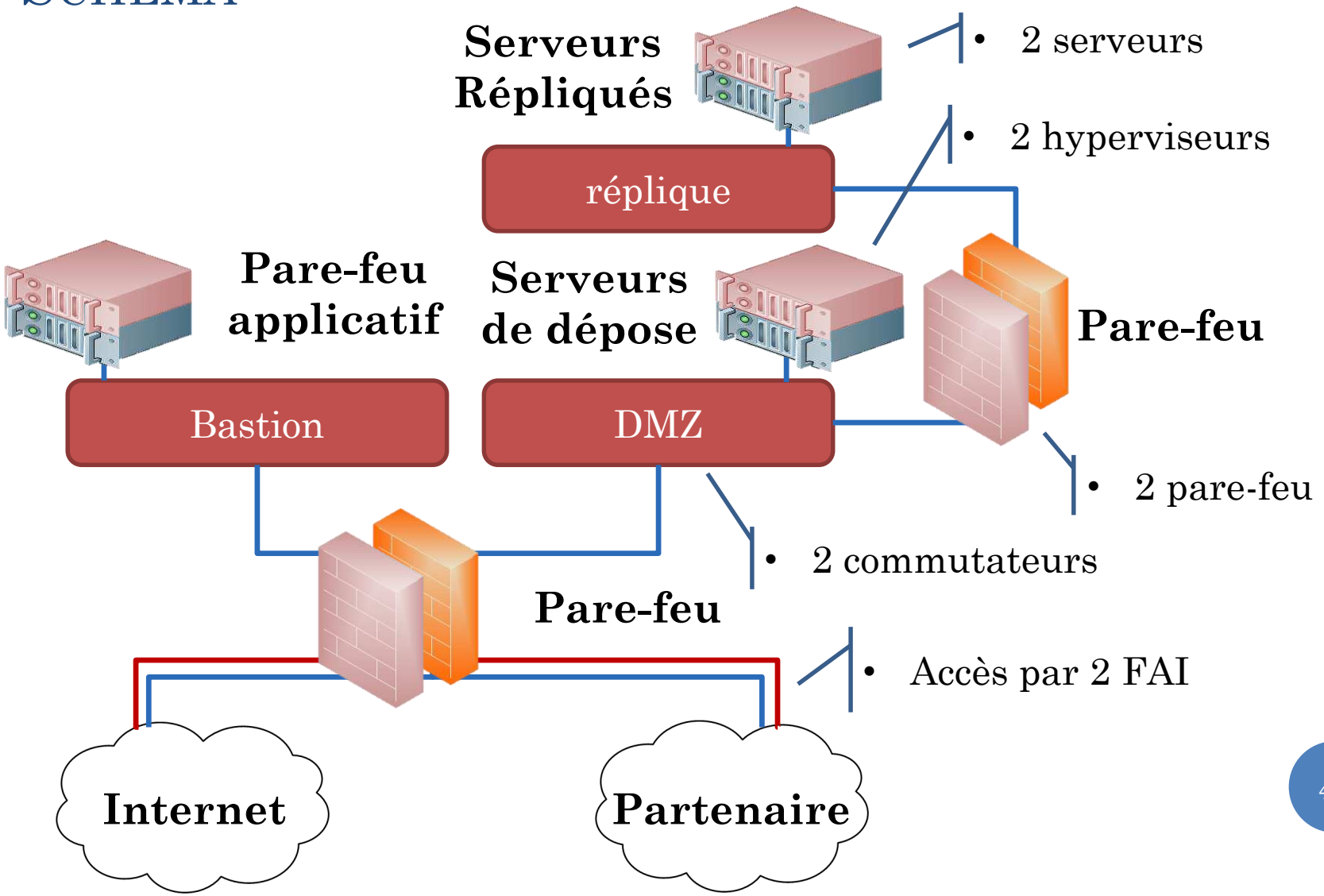
- Double accès Internet / partenaire par 2 FAI
- → Répartition de charge ou mise à jour du DNS

- Taux de service 99,99 % (~1 heure/an)
- → Remplacement à froid du matériel

- Taux de service 99,999% (~5 minutes/an)
- → Remplacement à chaud du matériel (doublement pare-feu, commutateurs, proxy, serveurs)

- Virtualisation des serveurs et / ou proxy (hyperviseurs)

V. Cas d'application
4. Disponibilité
Schéma

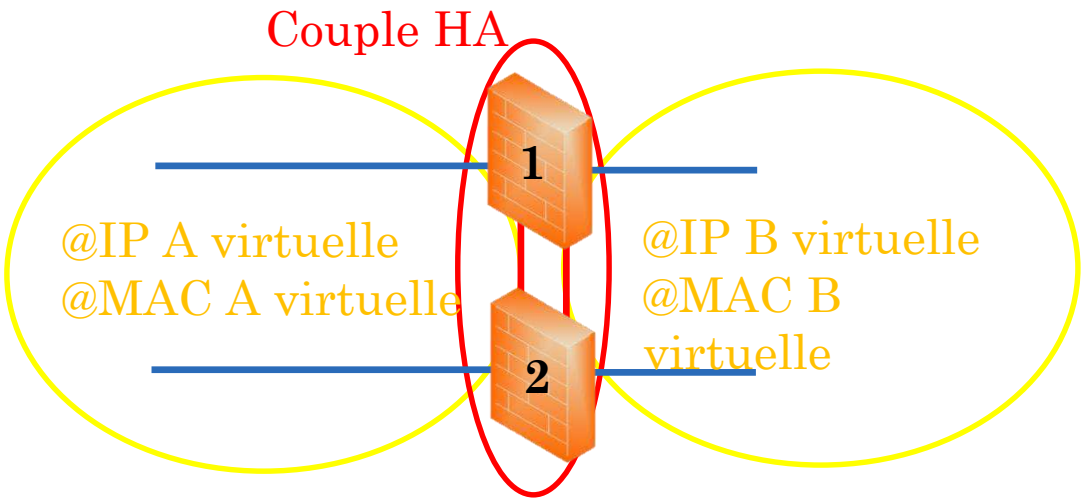


4. Disponibilité

Haute Disponibilité (HD) / High Availability (HA)

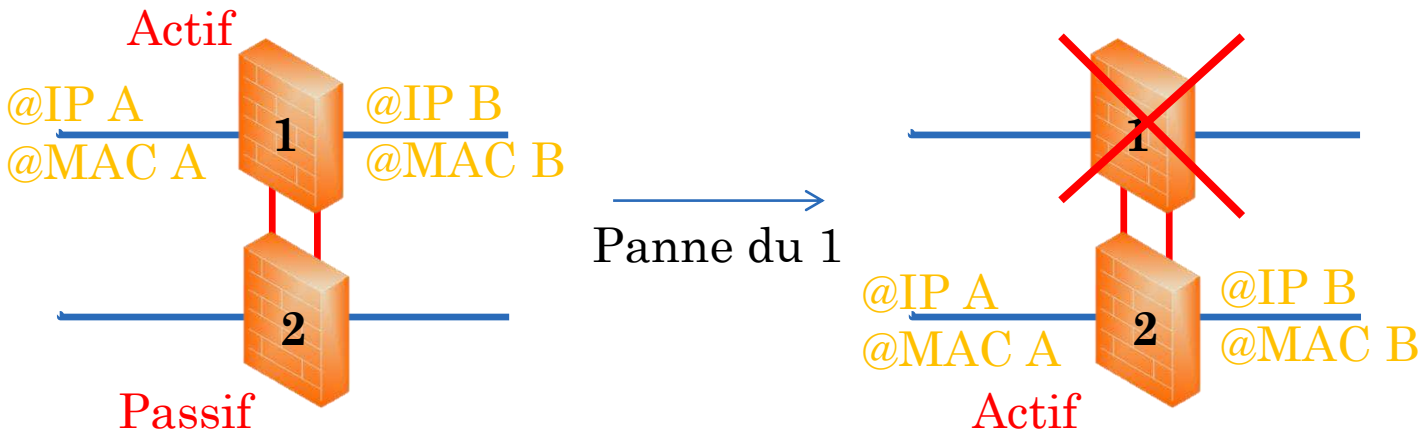
- Principaux modes HA :
  - **Actif / Passif** : Une seule machine transfère de la donnée à un instant donné dans le couple.
  - **Actif / Actif** :
    - Plusieurs machines actives à un instant donné.
    - Correspond à du loadbalancing.
  - Il existe plusieurs cas au-delà de 2 machines dans le cluster.

- Un couple HA utilise une @IP et une @MAC virtuelle
- Election distribuée de l'unité active
- Plusieurs protocoles : VRRP, HSRP, CARP, heartbeat et d'autres propriétaires
- Existe pour les pare-feu, proxys, serveurs



4. Disponibilité

Haute Disponibilité (HD) / High Availability (HA)



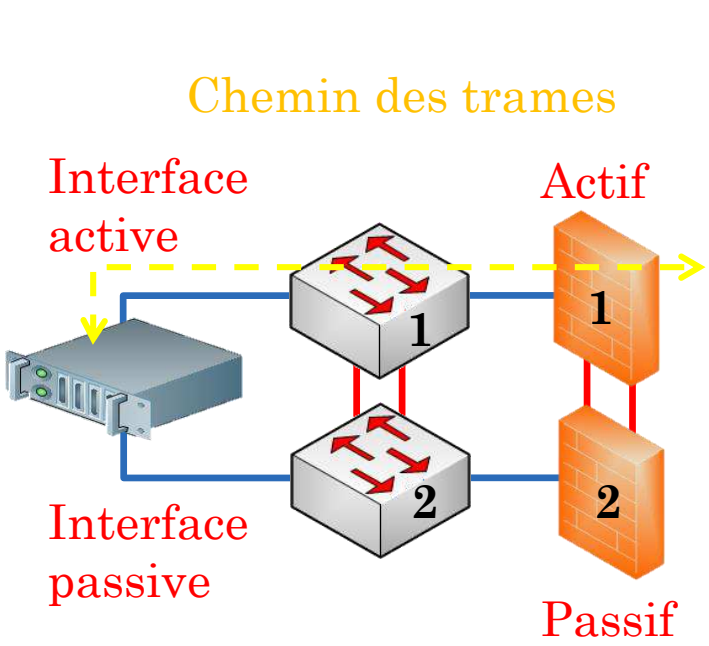
Split Brain

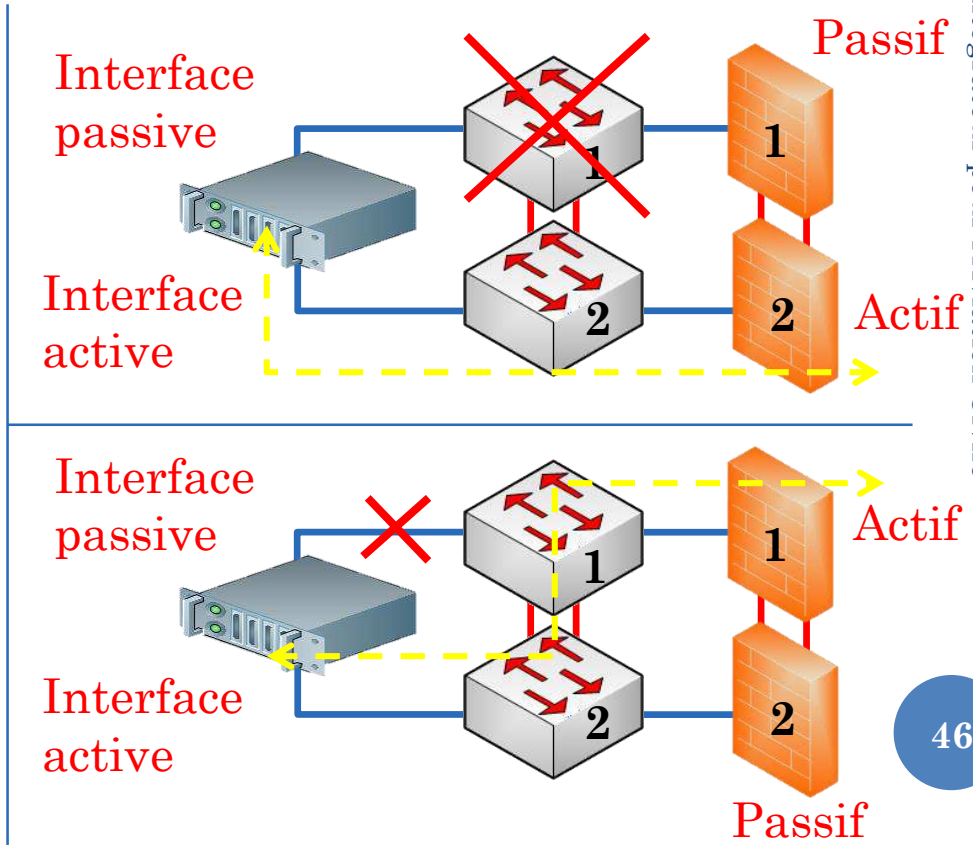
- Se caractérise par la présence sur le réseau de deux unités actives
- Deux @IP et @MAC sur le réseau au même moment, ça peut faire mal !!!
- → Attention à ne pas couper les liens HA (bien les identifier avant toute opération)
- → Il est conseillé d'avoir 2 liens HA

- Conseil : utilisé un câble d'une autre couleur

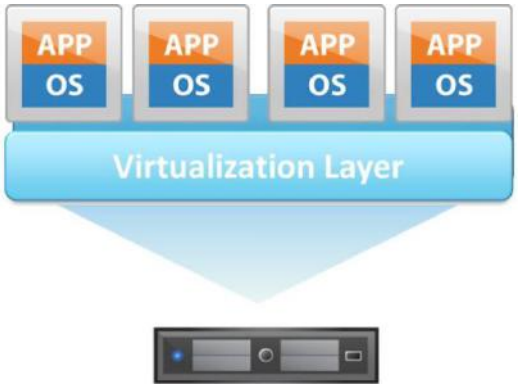
4. Disponibilité
Double raccordement

- Haute disponibilité des commutateurs
  - Mise en pile : par câble spécial ou LACP (agrégation de liens)





V. Cas d'application
4. Disponibilité Virtualisation



Avantages

- Economique
- Modulaire
- Restauration simplifiée
  → Reprise d'activité rapide
- Evolutivité
- Allocation dynamique des ressources
- Certains produits uniquement virtualisés

Inconvénients

- Point de défaillance commun
  → Doubler les hyperviseurs
- Ajoute du code
  → Plus de vulnérabilités
- Matériel plus cher à l'achat
- Composant supplémentaire à administrer

V. Cas d'application
5. DoS
Besoins

Besoins :

- Se protéger du déni de service

- Virtualisation
- DNS balancing sur les différents FAI
- Bloquer au niveau des pare-feu frontaux
- → limiter une IP à un certain nombre de connexions
- → limiter le nombre de connexions semi-ouvertes
- Mise en cache au niveau des proxys
- Duplication de l'architecture sur un autre site

6. Détection d'intrusion

Besoins

Besoins :

- Détecter les comportements anormaux
- Se mettre en capacité de détecter une attaque
- Se mettre en capacité d'analyser une attaque à posteriori

- Supervision de l'architecture
- → Mise en place d'un serveur de supervision

- Récupération des logs des équipements
- → Synchronisation NTP pour la datation des logs

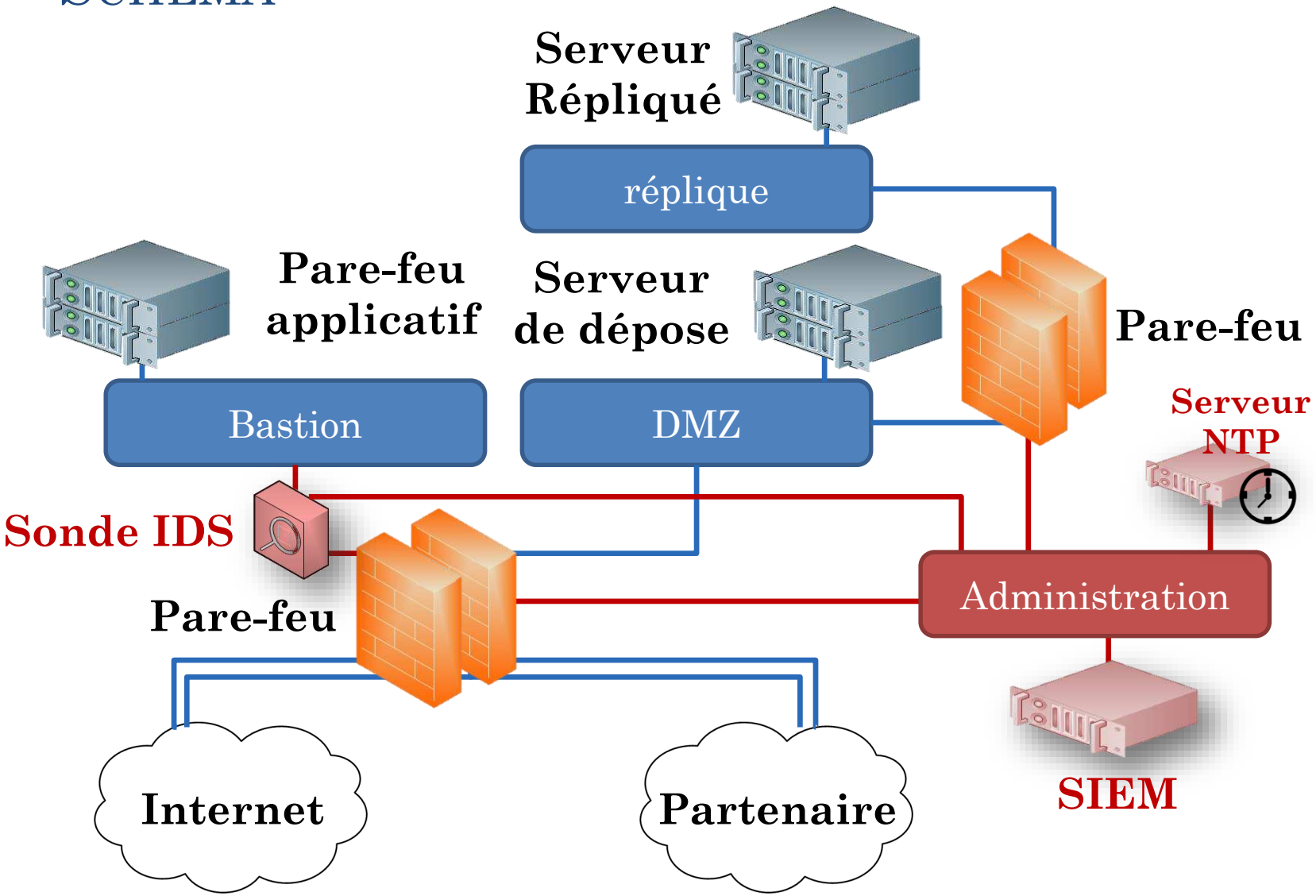
- Analyse et corrélation des logs

- Intrusion Detection System

- Vérification d'intégrité des systèmes (cf. durcissement système)

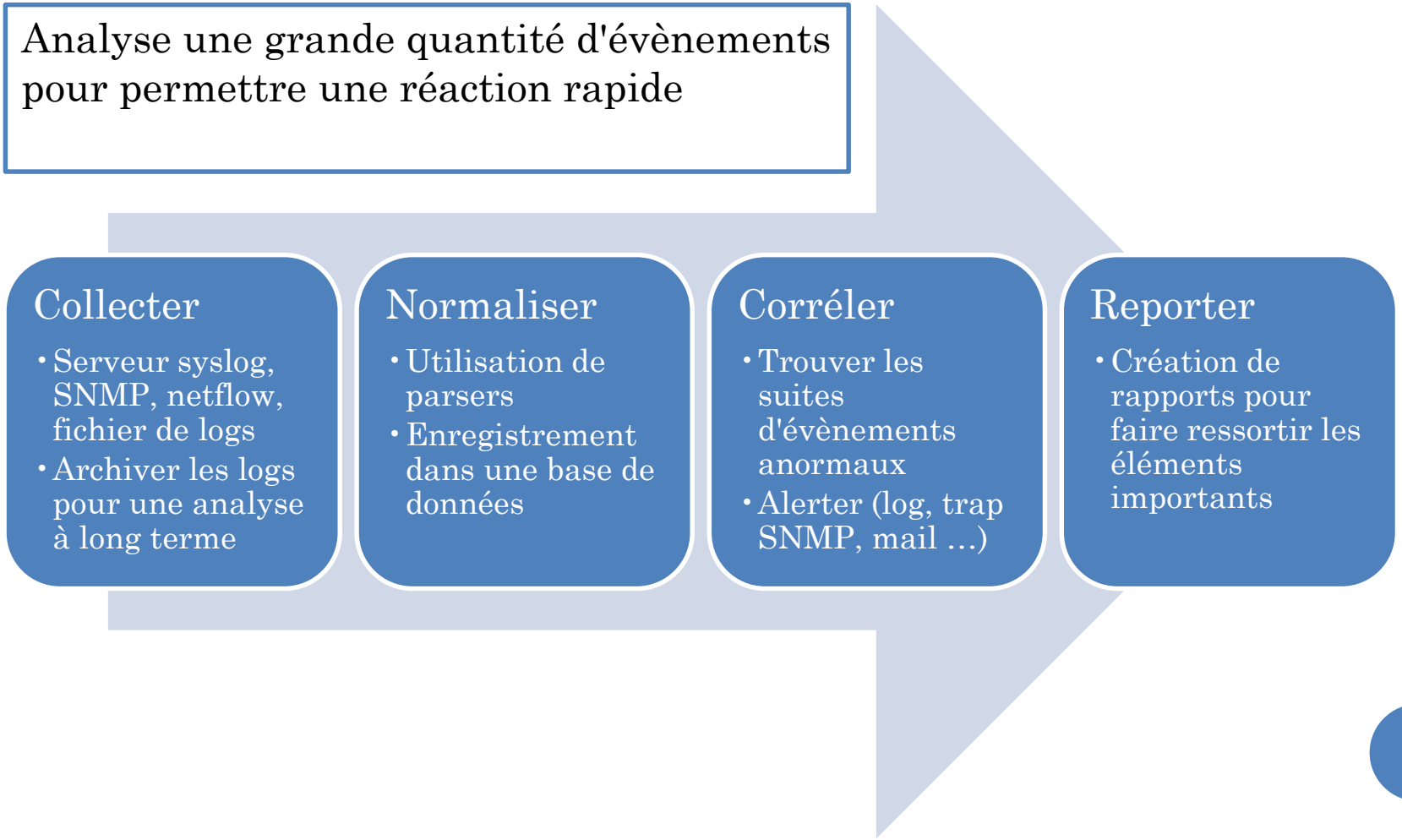
6. Détection d'intrusion

Schéma



V. Cas d'application
6. Détection d'intrusion
SIEM (Security Information Event Management)

Analyse une grande quantité d'évènements pour permettre une réaction rapide



V. Cas d'application
6. Détection d'intrusion
Supervision

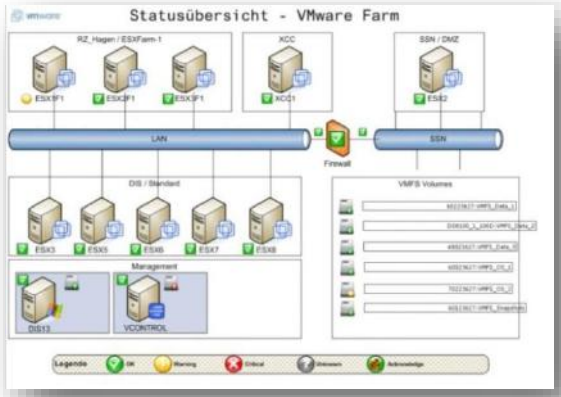
Objectifs

- Connaitre l'état de ses systèmes en "temps réel"

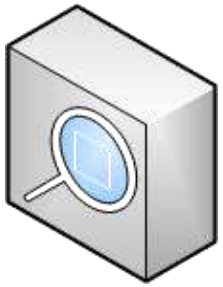
- A défaut d'empêcher une attaque, la détecter le plus vite possible
- Permet une analyse rapide de la situation
- Permet une reprise d'activité plus rapide

- Un protocole de prédilection : SNMP
  - SNMP v1 et v2 : nom de communauté en clair
  - **SNMP v3** : authenticité, confidentialité (AES128/DES) et intégrité (SHA1/MD5)
  - Communauté ou utilisateur en **lecture seule** ou lecture écriture (ro/rw)
- Pool (UDP/161) / Trap (UDP/162)
  - **Privilégier le pool** car assurance de connaitre l'état réel
  - Un trap peut se perdre ou peut ne pas être émis
- Exemple :
  - cas de panne électrique d'un équipement
    - pas de dernier souffle pour envoyer un trap
  - Trap au milieu d'une congestion

- Synoptiques



6. Détection d'intrusion
IDS / IPS



Objectif

- Détecter les comportements suspects sur le réseau

- IDS : non bloquant
- IPS : bloquant (risqué en cas de faut positif)

- Plusieurs types :
  - NIDS (Network)
    - Dans les pare-feu
    - Appliance dédiée
  - HIDS (Host) : Directement sur un hôte

- Très consommateur en ressource (regex/contextes)
  - → Débit de traitement très limité (goulot d'étranglement)
- Demande beaucoup de temps de configuration (quasi permanent)
  - → Les seuils de détection doivent suivre l'évolution du trafic
- Pas très utile si personne n'analyse et n'est capable de réagir rapidement

V. Cas d'application
6. Détection d'intrusion
Deep Packet Inspection (DPI)

Objectif :

- Analyser le trafic en profondeur (conjointement avec IDS)
- Retracer un incident / attaque au niveau de plus bas
- DLP : Data Leak Prevention
- Par exemple capable de reconstruire une session de surf sur Internet

Prérequis :

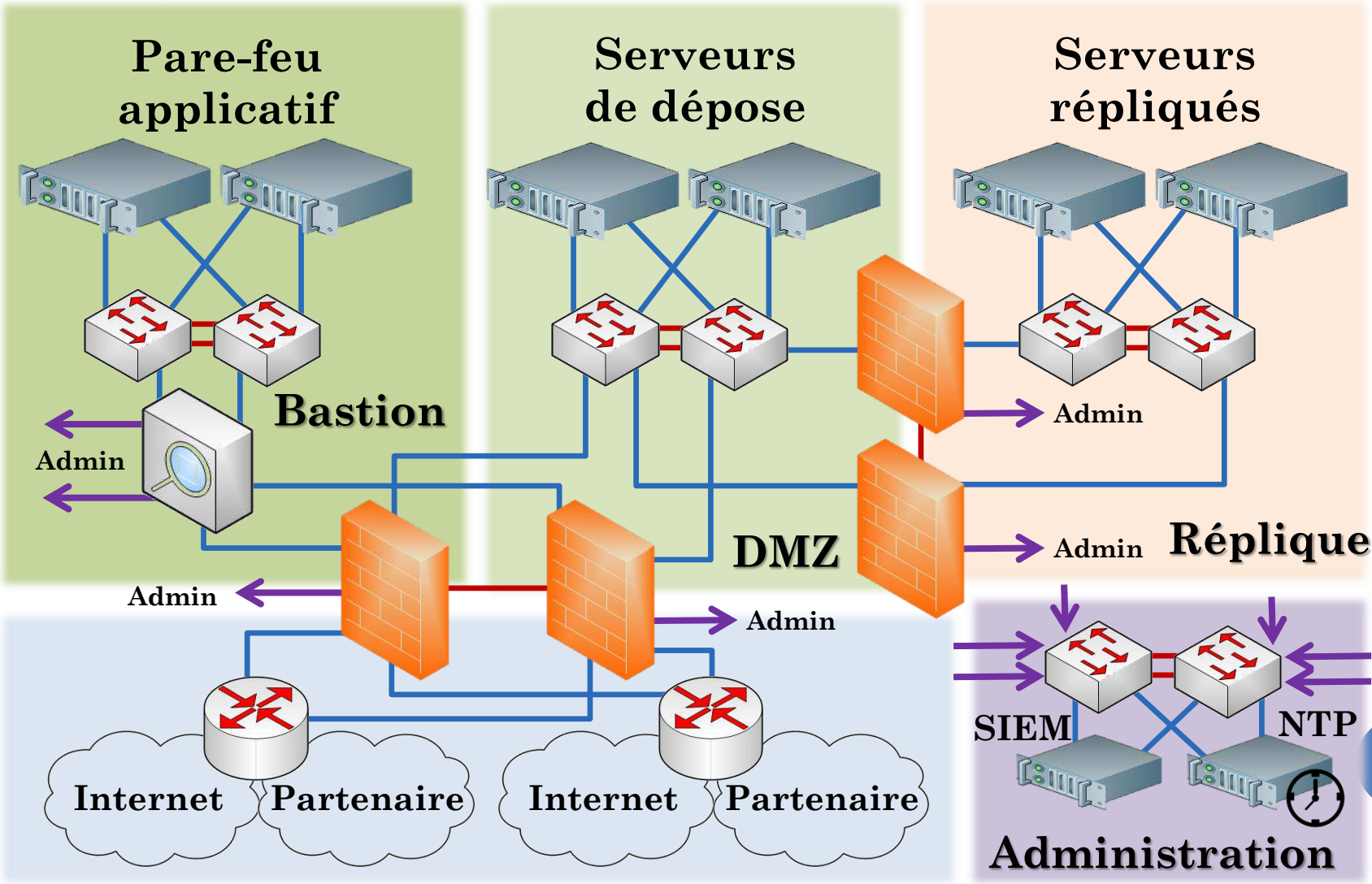
- Collecter toute l'information sur le réseau (capture réseau)
- → mirroring / SPAN port sur les commutateurs
- → TAP (Test Acces Port) : recopie du signal Ethernet
- Capacité de rétention importante (gourmand en ressources, x10 sur les logs)
- Sur dimensionner les liens

Limitations :

- Chiffrement (proxy SSL)
- DoS
- Faible temps de rétention (quelques jours) → l'attaque doit être détectée rapidement
- Stéganographie

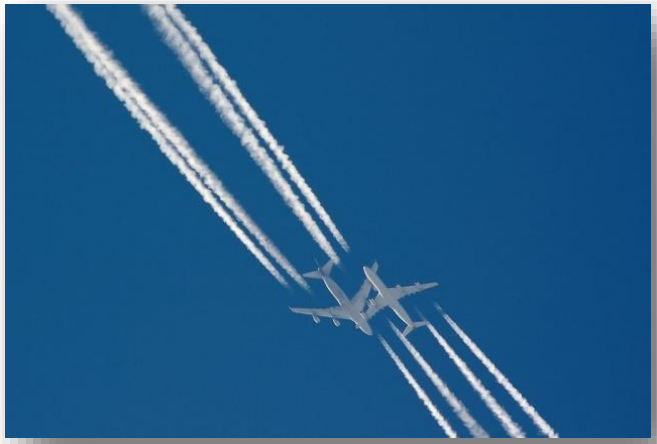
- Vie privée : Collecte de masse ≠ surveillance de masse

V. Cas d'application
Schéma physique global



Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. **Durcissement système**
VII. Intégration système
VIII. Cadre organisationnel
IX. Conclusion



VI. Durcissement système
Techniques de base

- Ensemble de techniques qui visent à rendre un système plus résistant aux attaques et qui le place dans les meilleures conditions pour assurer sa mission avec la meilleure disponibilité possible

- Réduction de la surface d'attaque

- Inclure dans le système uniquement ce qui est nécessaire (uniquement le code nécessaire pour rendre le service attendu)
- Tout code est potentiellement vecteur de faille
- Principe du "présent uniquement si nécessaire"

- Limiter les droits des utilisateurs :
  - privation de shell
  - droits sur l'arborescence (/var/log, /etc, /root, /bin, /sbin, /usr …)
  - Appartient à des groupes limités en droit

VI. Durcissement système
Techniques liées aux utilisateurs

- Complexité minimale sur les mots de passe (cracklib : complexité et dictionnaire)
- Durée de vie définie pour les mots de passe

- Limiter le nombre d'utilisateurs au strict nécessaire

- Dédier un utilisateur système pour chaque service
- Limiter les droits donnés aux programmes (en les exécutant avec un utilisateur bridé)

- Limiter le recours à l'utilisateur root
- Interdire les connexions directes par l'utilisateur root (login prévisible)

Bonnes pratiques

- Favoriser des méthodes d'authentification multi-facteur
- Ne pas autoriser les utilisateurs "groupe"

VI. Durcissement système
Techniques liées aux services

- Limiter les accès externes à quelques services et quelques utilisateurs aux droits limités
- Mettre en place du bannissement en cas d'échecs de connexion répétés

- Limiter les services qui s'exécutent

- Limiter les services accessibles de l'extérieur / de l'intérieur (nmap/netstat)
- Réduire la surface d'attaque réseau

- Limiter les informations sur la version et le programme qui rend le service (mode production)

- Limiter les services trop bavards (il suffit de regarder ce qui sort d'une machine)
- Exemple : MaJ, rapport de crash, découverte réseau (Avahi), Netbios/SMB …

- Limiter la dérive système, l'accumulation non maitrisée (quota, rotation, purge)
- Exemple : logrotate, coredump, /home, /var/www …

- Durcir les couches réseau (TCP Wrapper, ARP statiques, routage statique, DNS, réponses ICMP)
- Configurer les options systèmes (syscontrol)

VI. Durcissement système Intégrité

Objectif :

- Détecter les modifications apportées à un système
- Détecter les intrusions en analysant régulièrement l'intégralité du système
- Garantir l'intégrité du système (garantie d'assez bas niveau)

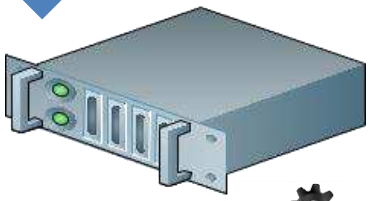
Paramètres enregistrés :

- Somme de contrôle
- Droits
- Dates (création, dernier accès, dernière modification)
- Inode
- Nombre de fichiers
- …

VI. Durcissement système
Intégrité - fonctionnement

1
- Un fichier de référence est généré à l'installation (quand le système est considéré comme intègre)
- Il est sauvegardé dans un lieu sûr pour analyse post mortem
- Certains logiciels fournissent des signatures de fichiers bien connus

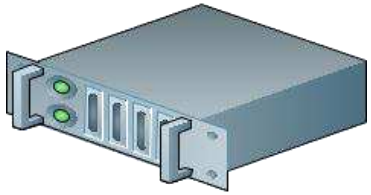
2
- Une analyse est effectuée régulièrement pour analyser les éventuelles modifications
- En cas de modification justifiée, la nouvelle base est considérée comme nouvelle base de référence



1

Vérification d'intégrité

Base de référence

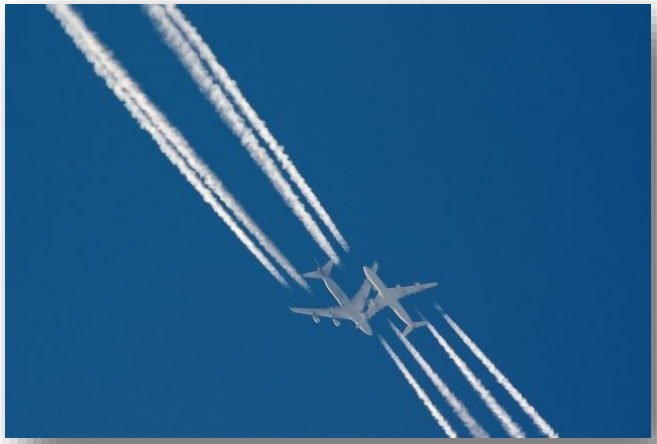


2

Base issue de
l'analyse du système

Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. **Intégration système**
VIII. Cadre organisationnel
IX. Conclusion

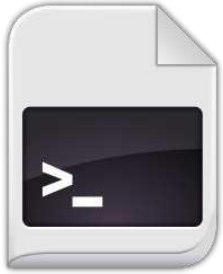


VII. Intégration système
Principes de base

Objectifs :

- Automatiser pour éviter les erreurs
- Accélérer la reprise d'activité
- Protéger l'utilisateur de sa méconnaissance en le guidant
- Uniformiser les systèmes pour rendre la maintenance plus aisée

- Toujours garder en tête le fragile équilibre : sécurité / fonctionnalité / facilité d'utilisation
- Le bon système pour les bons besoins
- Automatisation de l'installation :
  - Outil : Preseed (Debian, Mint, Ubuntu …) kickstart (RedHat, Fedora, CentOS …)
  - Formatage
  - Configuration réseau
  - Sélection des paquets (apt/rpm/ports/…)
  - … tout ce qui est demandé lors d'une installation classique
  - **Durcissement** (scripts)
  - Personnalisation de l'environnement (scripts)
  - Configuration de l'accès d'administration
  - Configuration des services
  - Création des utilisateurs
  - Modifications des mots de passe (TOUS, on ne laisse pas de mot de passe par défaut)

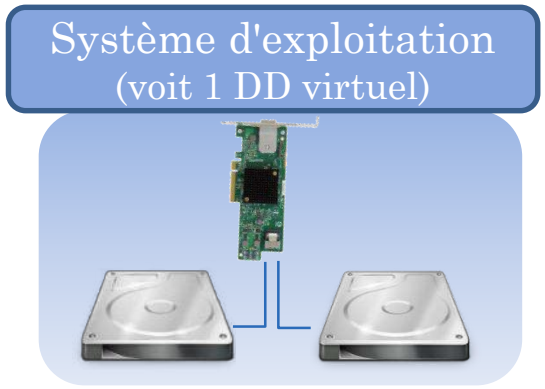


VII. Intégration système Disponibilité

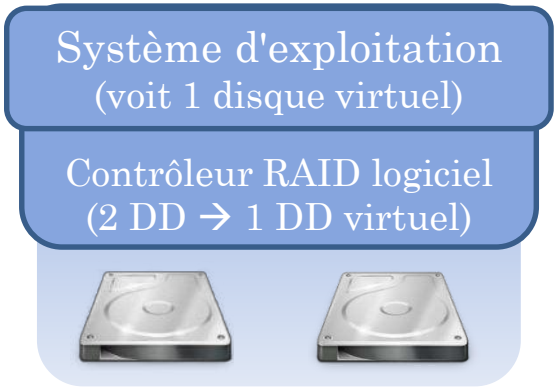
Disponibilité système :

- Dupliquer la donnée :
  - système de fichier réparti
  - base de données répartie
- Mise en HA : HeartBeat (HB)
  - Partage d'adresse similaire au VRRP
- Superserveurs : relance un service en cas de problème (xinetd)
- RAID : tolérer des pannes sans perte de données

RAID



RAID software



VII. Intégration système Debian

- Paquets précompilés (système APT)
- Communauté très développée
- MaJ fréquentes
- Relativement sécurisé / stable
- Pérennité du projet
- LTS (Long Term Support)

- Ne sacrifie pas l'évolutivité pour la sécurité
- Très répandu
- Encore plus répandu par héritage (Ubuntu, Mint, Kali, DVL …)
- Pas de support commercial, contrairement à RedHat

VII. Intégration système
Système de dépôts (APT)

- Plein de miroirs (pas forcément sous l'autorité de la communauté)
- Garantie sur l'origine du paquet (signature numérique)

- Clé publique officielle de la version livrée dans le CD d'installation (apt-key dans **trusted.gpg**)
- Signature du fichier release : http://ftp.fr.debian.org/debian/dists/wheezy/**Release.gpg**
- Descriptif des fichiers du dépôt (index) : http://ftp.fr.debian.org/debian/dists/wheezy/**Release**
  - Contient le haché de tous les fichiers du dépôt : MD5, SHA1, SHA256
  - On peut avoir confiance dans le contenu des infos des fichiers du dépôt par vérification du hash

Fichier "Release"

- Origin: Debian
- …
- Version: 7.9
- Codename: wheezy
- Date: Sat, 05 Sep 2015 11:44:23 UTC
- Architectures: amd64 armel armhf i386 ia64 kfreebsd-amd64 kfreebsd-i386 mips mipsel powerpc s390 s390x sparc
- Components: main contrib non-free
- Description: Debian 7.9
- Released 05 September 2015
- MD5Sum:
  - **e28e71c16cac0c411bf5b2e461dff972 304063644 Contents-amd64**
  - **ea4195b21ab485e59b9ef30357e709ca 21606550 Contents-amd64.gz**
  - …

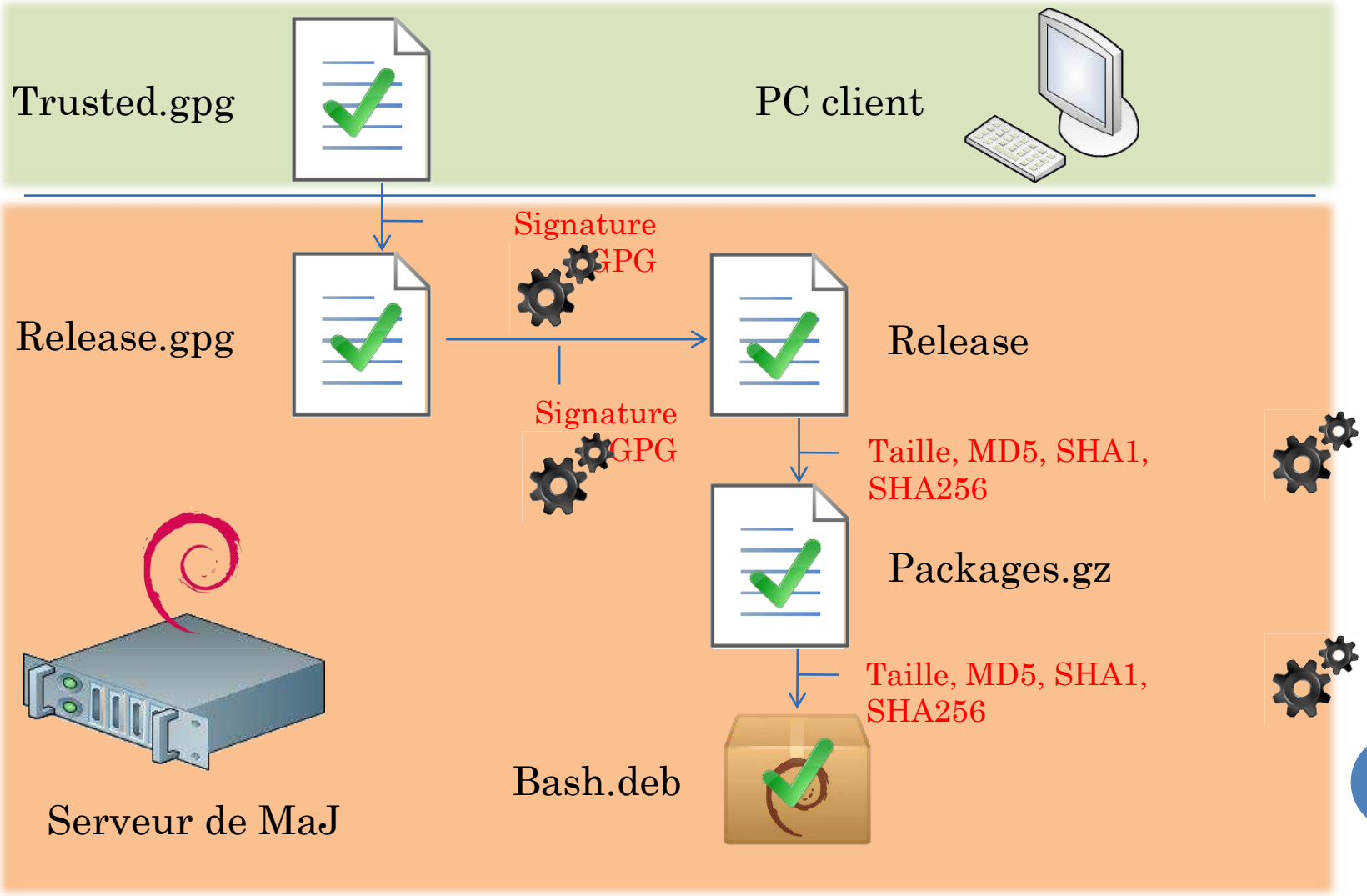
VII. Intégration système
Système de dépôts (APT)

- Toutes les propriétés des paquets sont dans : http://ftp.fr.debian.org/debian/dists/wheezy/main/binary-i386/Packages.gz
  - on peut avoir confiance dans le contenu des paquets après vérification des propriétés (nom, taille, hachés)

Exemple : Bash

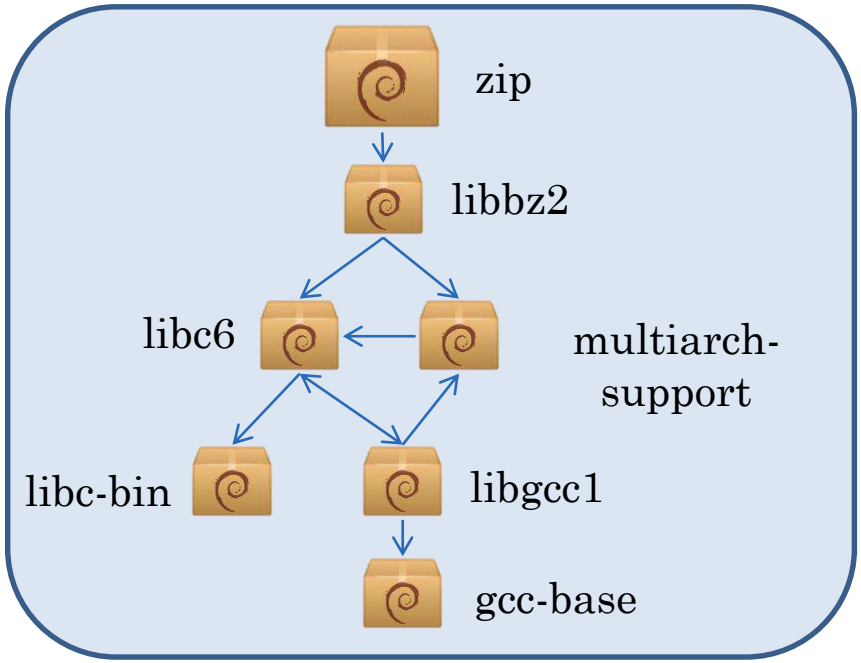
- Package: bash
- Version: 4.2+dfsg-0.1+deb7u3
- Installed-Size: 3902
- Maintainer: Matthias Klose doko@debian.org
- Architecture: i386
- Replaces: bash-completion (<< 20060301-0), bash-doc (<= 2.05-1)
- **Depends: base-files (>= 2.1.12), debianutils (>= 2.15)**
- Pre-Depends: dash (>= 0.5.5.1-2.2), libc6 (>= 2.11), libtinfo5
- Recommends: bash-completion (>= 20060301-0)
- Suggests: bash-doc
- Conflicts: bash-completion (<< 20060301-0)
- Description: GNU Bourne Again Shell
- […]
- **Filename: pool/main/b/bash/bash_4.2+dfsg-0.1+deb7u3_i386.deb**
- **Size: 1472464**
- **MD5sum: 0fd27715e269feda81dcd59fb79665f1**
- **SHA1: 68d4446dc31c4fc1555d6f6d432f2ccd31ffda4e**
- **SHA256: e69d34a618a00ec21b64c361eec491cb034336ca790668a42409ee39bf96ff78**

VII. Intégration système
Système de dépôts (APT)



VII. Intégration système
Système de dépôts (APT)

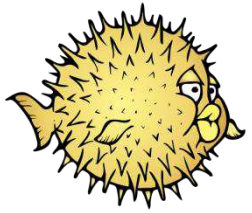
- Paquets : fichier ".deb" (tar.gz le plus souvent)
- Contient :
  - Binaires
  - Sources
  - Pages man
  - Fichiers de configuration
  - …



- Arbre de dépendances
  - Exemple : **zip**
  - ATP abstrait la complexité
    - apt-get install zip

- Intégrité du contenu du CD (paquets .deb en grande partie)
  - md5 de tous les fichiers du CD
  - Auto-vérification du média d'installation

VII. Intégration système OpenBSD



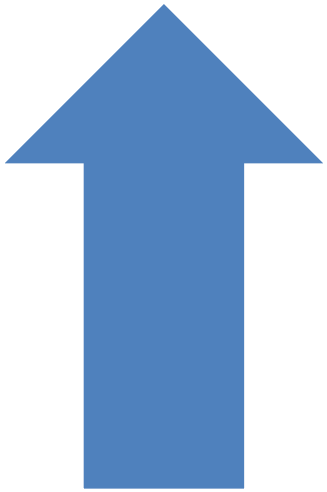
OpenBSD

- Philosophie : Sécurisé par défaut

- Durcissement fait
- Facilite l'intégration
- Très utilisé pour les systèmes sécurisés
- Paquets précompilés (système de port)

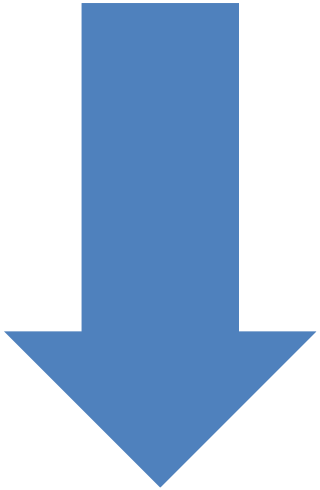
- Austère
- Maj de sécurité requièrent recompilation du système (long et interruption de service)

VII. Intégration système Diversité



Avantages

- Favoriser la diversité pour éviter les SPoF
- Requiert des connaissance mutli-système pour parvenir à mener une attaque complète
- L'un des seuls remède efficace aux zeroday

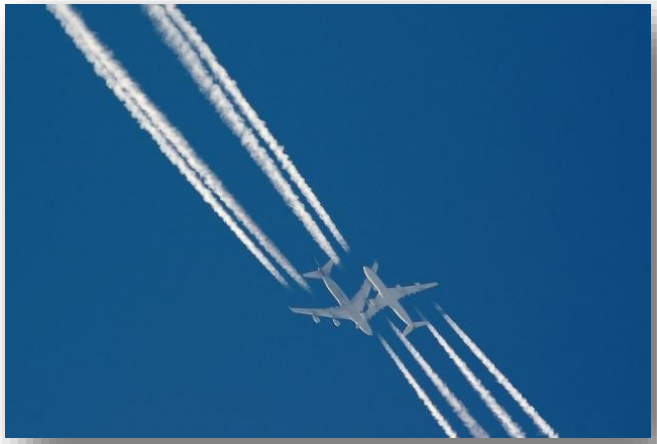


Inconvénients

- Il n'y a qu'un ensemble fini de systèmes
- Pas de capitalisation
- Nécessite plus de ressources :
  - Un effort de formation
  - Un effort de maintenance
  - Un effort pour l'évolution

Plan

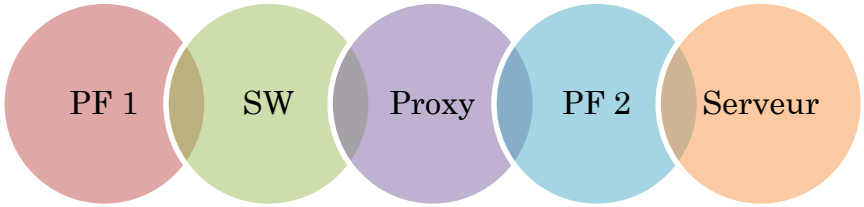
I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. **Cadre organisationnel**
IX. Conclusion

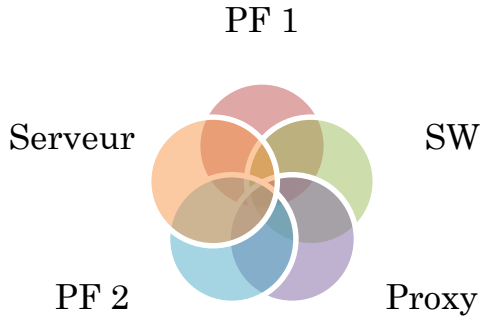


VIII. Cadre organisationnel
Gestion des vulnérabilités

1. Vérifier si les systèmes possèdent des vulnérabilités connues
   - Détecter les versions des systèmes par scan (actif/passif) ou inventaire
   - S'appuyer sur les bases de connaissance de vulnérabilité
     - CVE : Common Vulnerabilities et Exposures
     - CERT : Computer Emergency Response Team

2. Vérifier si l'ensemble des vulnérabilités expose à un risque





3. Patcher les systèmes pour éliminer le risque lié à la vulnérabilité

❖ <u>Limitation</u> : ne protège pas des vulnérabilités non connues

VIII. Cadre organisationnel
AUDIT

- Audit : Vérifier la conformité du SI à une référence

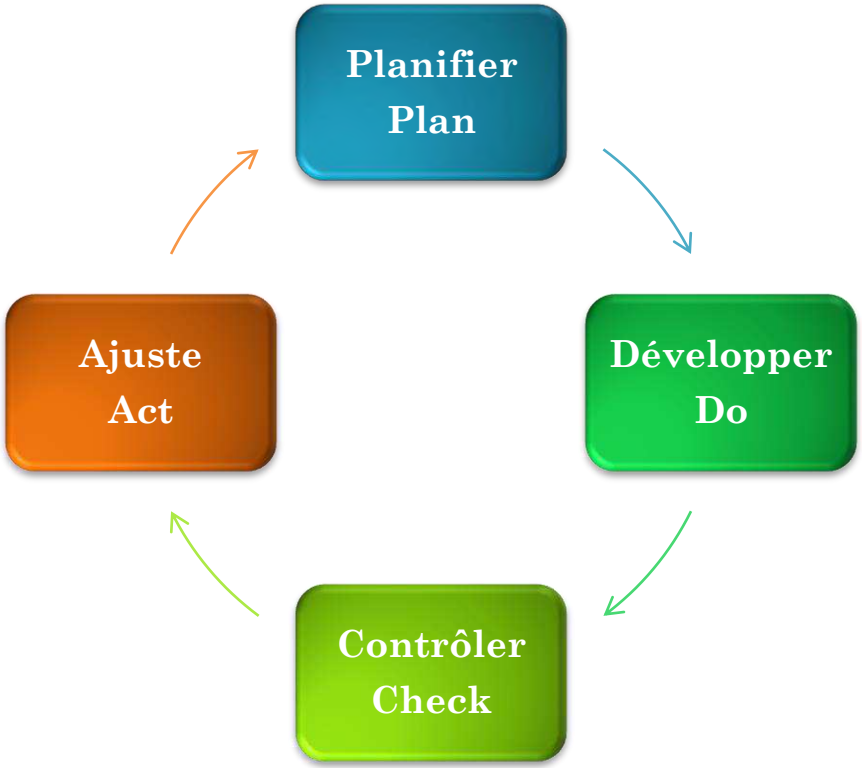
- Audit organisationnel : regarde la cohérence avec des normes (ISO 2700X, PCI-DSS…)
- Audit technique : test de pénétration (pentest : vérifier les mécanismes de sécurité en se mettant à la place d'un attaquant)

- évalue la non-conformité, identifie des risques (outils : EBIOS, MARION, MEHARI …)

- Termine la roue de Deming (ISO 2700X)
  - principe d'amélioration continue

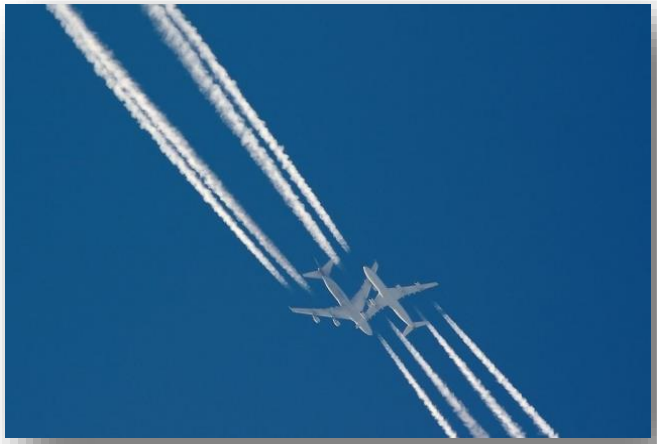
VIII. Cadre organisationnel Audit et SMSI

- SMSI : Système de Management de la Sécurité de l'Information
- Principe d'amélioration continu (PDCA / PDSA)
- Défini dans la norme ISO 27001



Plan

I. Présentation
II. Contexte / Enjeux
III. Aspects réglementaires
IV. Architecture réseau
V. Cas d'application
VI. Durcissement système
VII. Intégration système
VIII. Cadre organisationnel
IX. **Conclusion**



IX. Conclusion
Cycle de vie d'une architecture sécurisée

Avant l'attaque

- Architecture : on construit sa défense, on se prépare à subir une attaque (durcissement, réplication …)
- Procédures : isolation, bannissement, PRA : Plan de Reprise d'Activité / DRP : Disaster Recovery Plan …

Pendant l'attaque

- Détecter l'intrusion (supervision, logs, intégrité, IDS)
- Limiter les impacts

Après l'attaque

- Avoir les moyens de retrouver l'attaquant (logs, intégrité, DPI, inforensic)
- La vie continue, il faut reprendre l'activité rapidement
- Reconstruire une défense solide face à l'attaque menée et à ses variantes

IX. Conclusion
Conseils

Conception

- Une attaque profite des cas limites non prévus ! (DoS, buffer overflow)
- → toujours voir le pire et le mal partout
- → la paranoïa est "saine" en sécurité
- Ne pas mettre d'œillères, toujours imaginer tous les cas d'attaque possibles

- Toujours garder en tête l'équilibre : sécurité/fonctionnalité/facilité d'utilisation
- La sécurité n'est jamais une fin en elle-même, elle n'est utile qu'à protéger ce qui a réellement de l'importance

Support

- En réseau, vérifier couche par couche (OSI)
- En système, ça n'est pas aussi simple, approche en couche moins évidente
  - PEBCAK : Problem Exists Between Chair And Keyboard
  - N'est pas la réponse à tout problème, mais en explique beaucoup

IX. Conclusion
En résumé

Ingénieur sécurité vs Hacker

- L'ingénieur perd toujours, car il a plus à perdre (de l'argent, des vies, une image)
- Il est plus facile de détruire que de reconstruire
- On peut seulement se préparer au mieux pour affronter une attaque

"There is no patch to human stupidity"

- Unique vaccin : formation contre l'ingénierie sociale
- L'ingénierie sociale est souvent plus simple que de s'attaquer au technique

Réseau vs Sécurité

- En interconnectant on prend toujours un risque, il s'agit de le réduire au minimum
- Après il faut l'accepter (RSSI ou PDG), à défaut vivre avec

Merci pour votre attention

Contact

- aurelien.bouzon@alumni.enseeiht.fr

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 »***

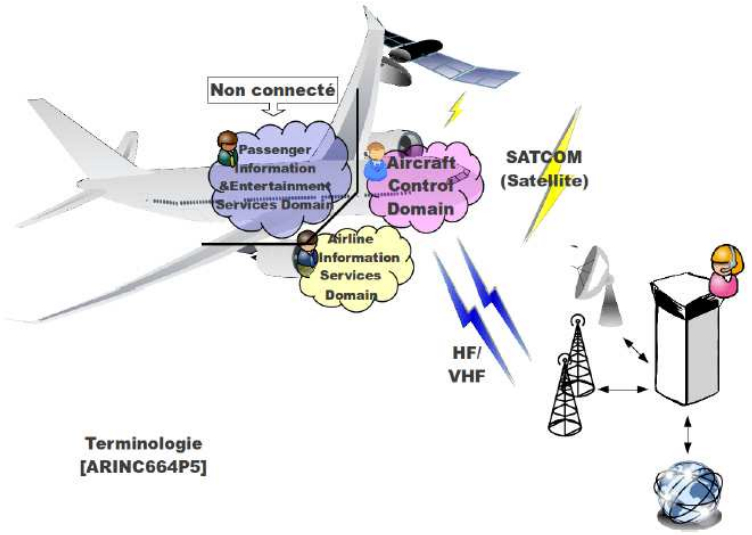
Plan de la présentation

- **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**

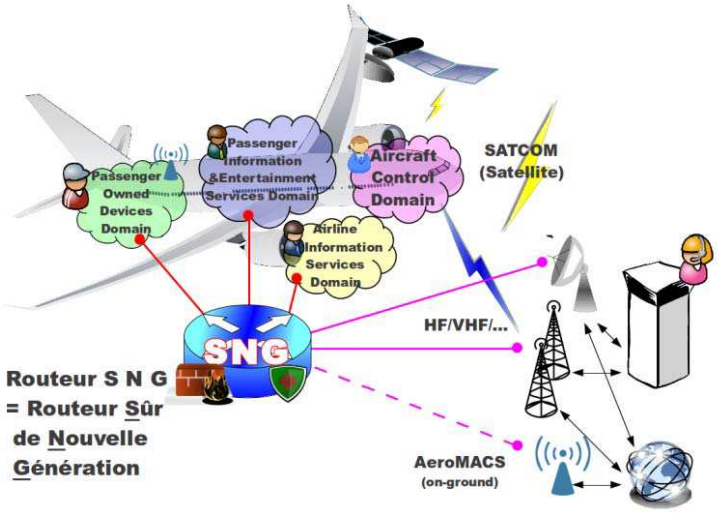
Plan de la présentation

- **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)

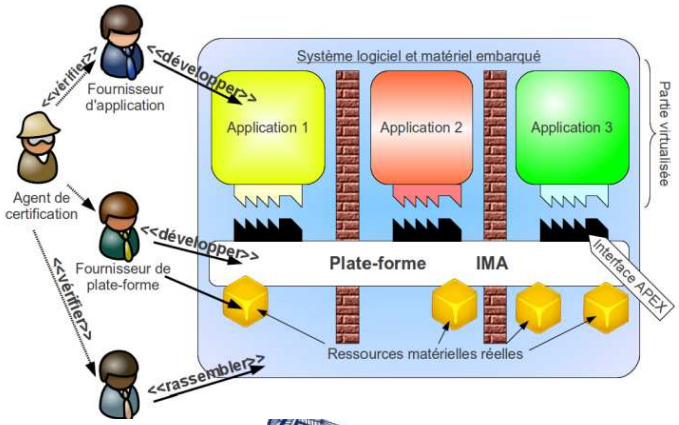
La sûreté est la propriété d'immunité du système, elle qualifie la capacité d'un système à gérer les menaces et dangers externes au système.
Synonymes : sécurité informatique (hors domaine du transport) ! Sécurité-immunité, «security» en Anglais.

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]

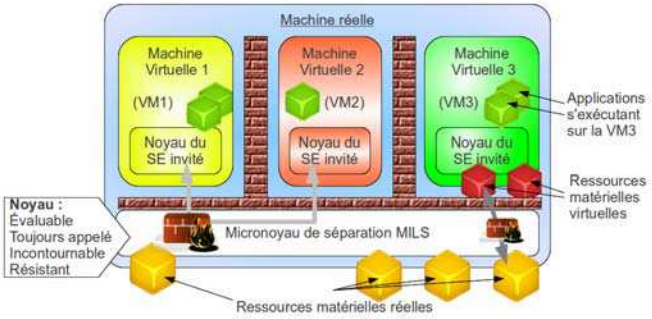
Norme définissant une **architecture** créée pour le **monde aéronautique**, en tenant compte des contraintes élevées de **sécurité**



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

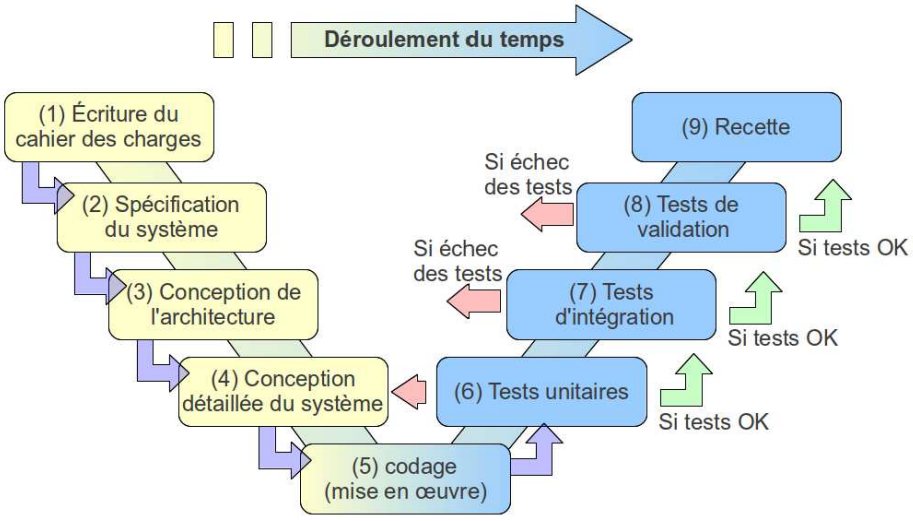
Sûreté : Évaluation

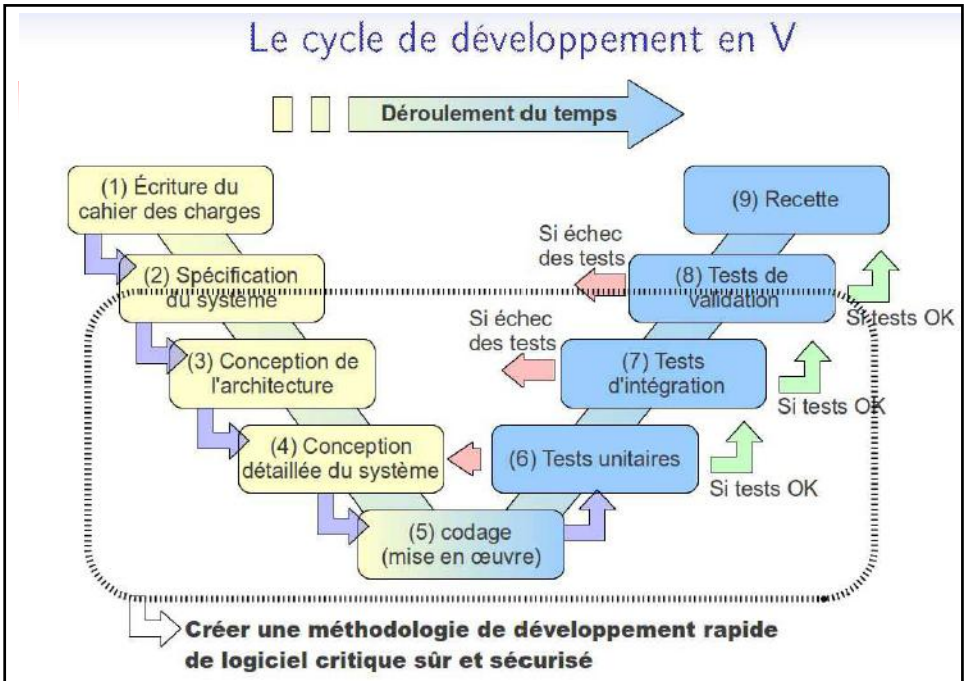
- [ISO 15 408] Critères Communs : norme utilisée pour évaluer la sûreté du routeur SNG
- Ecriture d'un **Profil de Protection** (PP) pour formaliser l'analyse et guider l'évaluation du Routeur SNG

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



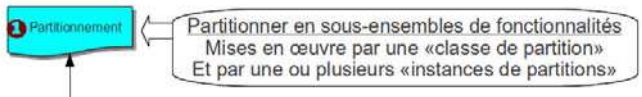


Objectifs

- 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

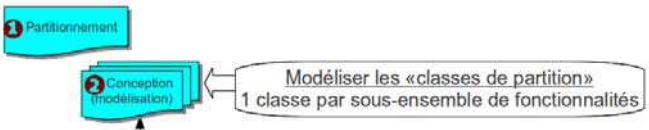
Développement rapide de logiciel critique sûr et sécurisé



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

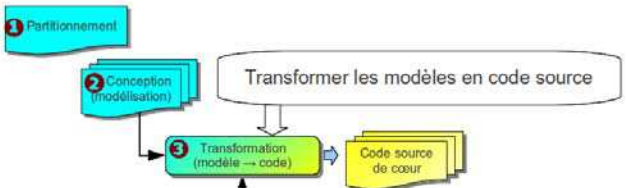
Développement rapide de logiciel critique sûr et sécurisé



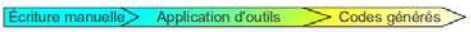
Usage de modèles :
+ Validation et correction au plus tôt (baisse des coûts)
+ Classes portables, réutilisables pour d'autres projets
+ Possible de créer des variantes dédiées au débogage
  ou au contrôle et de facilement intervertir entre les versions
+ Compatible avec la certification en suivant le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

Une méthodologie générique en sept étapes

Développement rapide de logiciel critique sûr et sécurisé

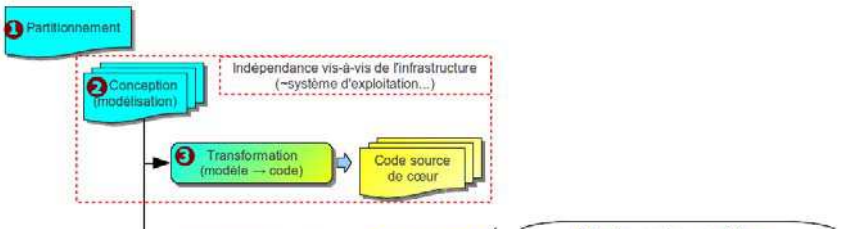


Transformation automatisée [Toom&al. 2010]
+ Rapidité de développement
+ Assurance que le code correspond parfaitement au modèle (pas d'erreur de conversion manuelle)
! Il faut valider l'outil de transformation



Une méthodologie générique en sept étapes

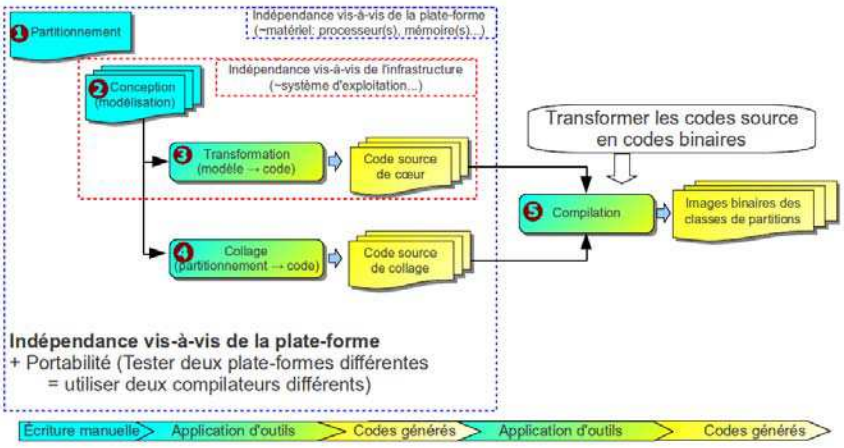
Développement rapide de logiciel critique sûr et sécurisé



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

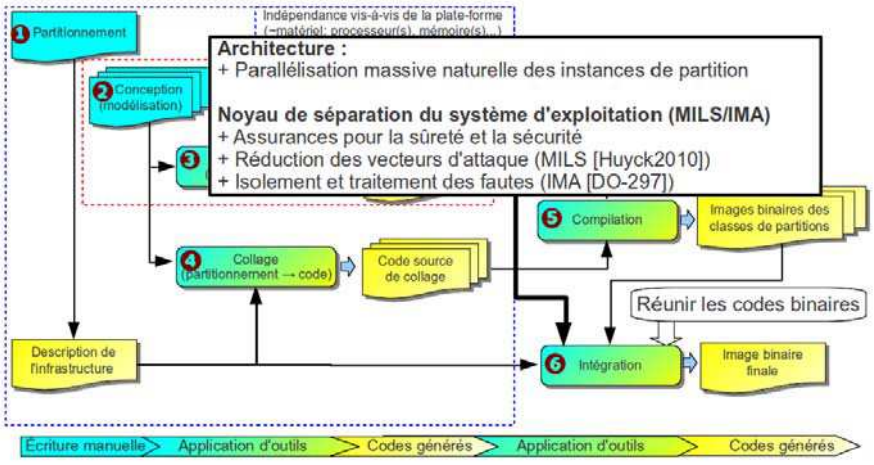
Une méthodologie générique en sept étapes

Développement rapide de logiciel critique sûr et sécurisé



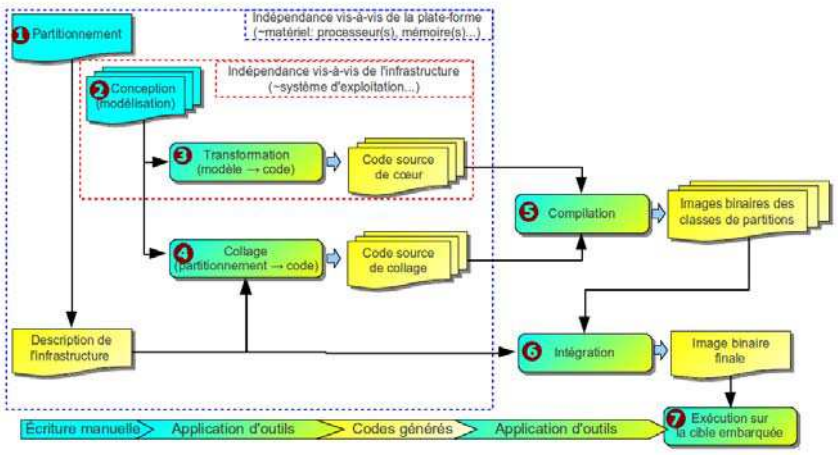
Une méthodologie générique en sept étapes

Développement rapide de logiciel critique sûr et sécurisé

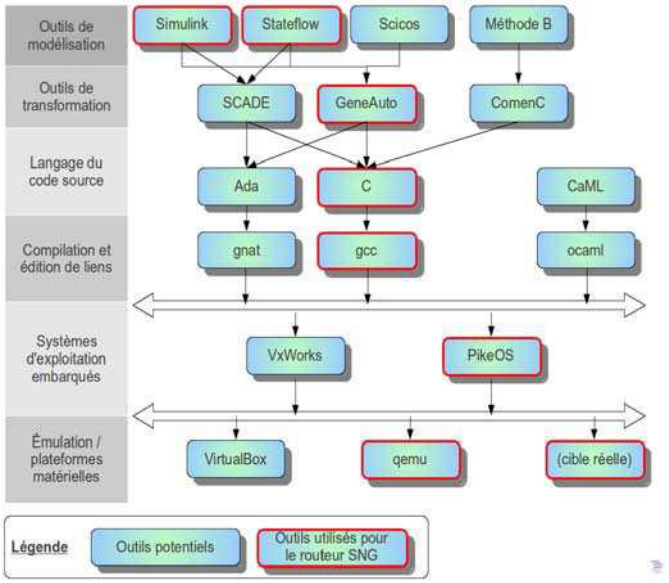


Une méthodologie générique en sept étapes [DASC11]

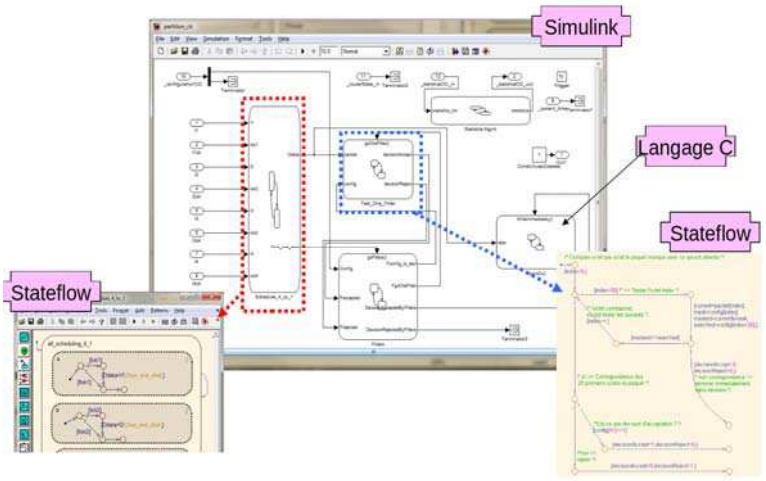
Développement rapide de logiciel critique sûr et sécurisé



Instanciation de la méthodologie



Utilisation de cette méthodologie



Plan de la présentation

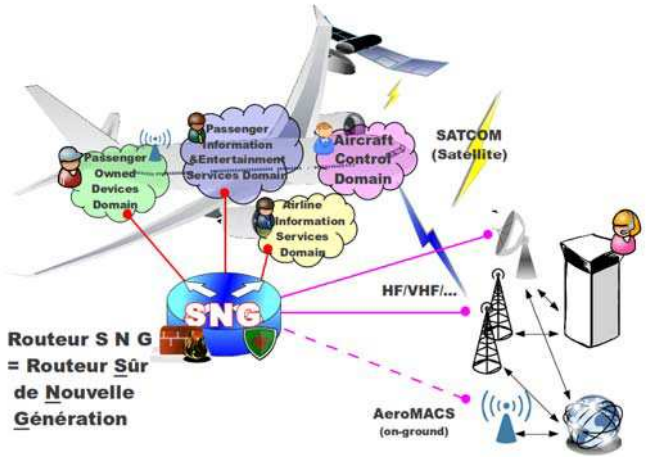
- **Introduction, définitions et contexte**
- **Section 1: exemple de méthode pour fusionner "security" et "safety"**
- **Section 2: exemples de solutions sures et/ou sécurisées pour l'aéronautique**
  - **Développement d'un routeur sur et sécurisé pour l'aéronautique**
  - **Un protocole d'auto-négociation 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**

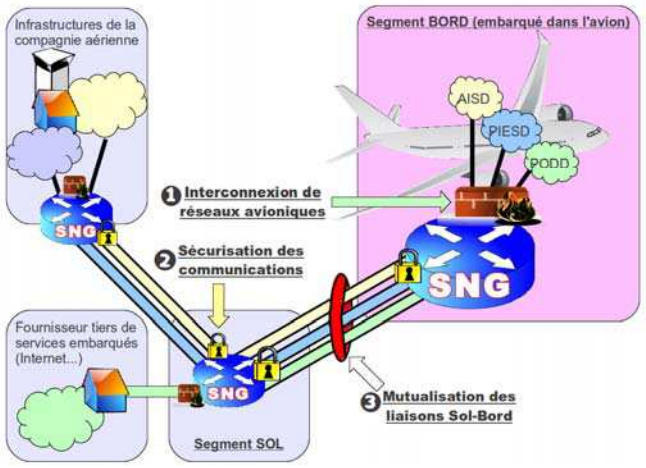
Intérêt d'un routeur embarqué Sûr de Nouvelle Génération

Interconnexion des réseaux avioniques



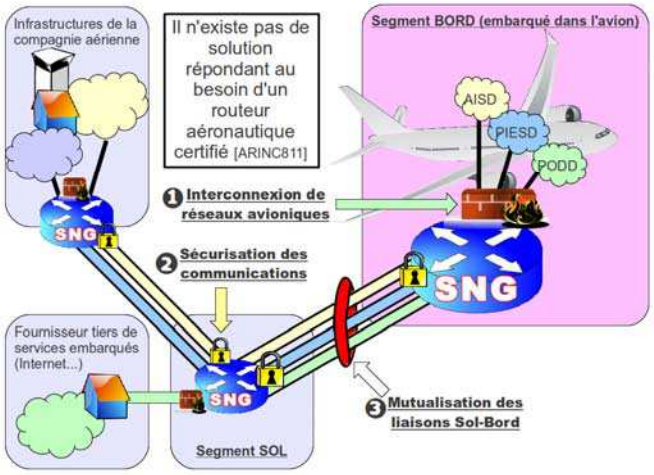
Intérêt d'un routeur embarqué Sûr de Nouvelle Génération

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

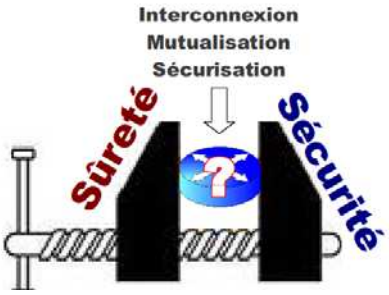
Amélioration des communications de données pour un réseau de communication contraint

- 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])

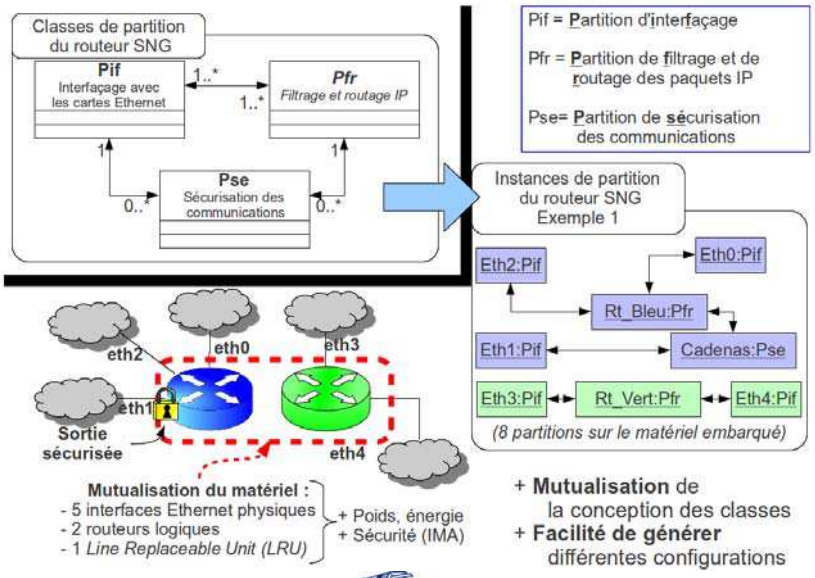
Vérification et validation de la sûreté et de la sécurité

Développement du routeur SNG : sûreté ET sécurité

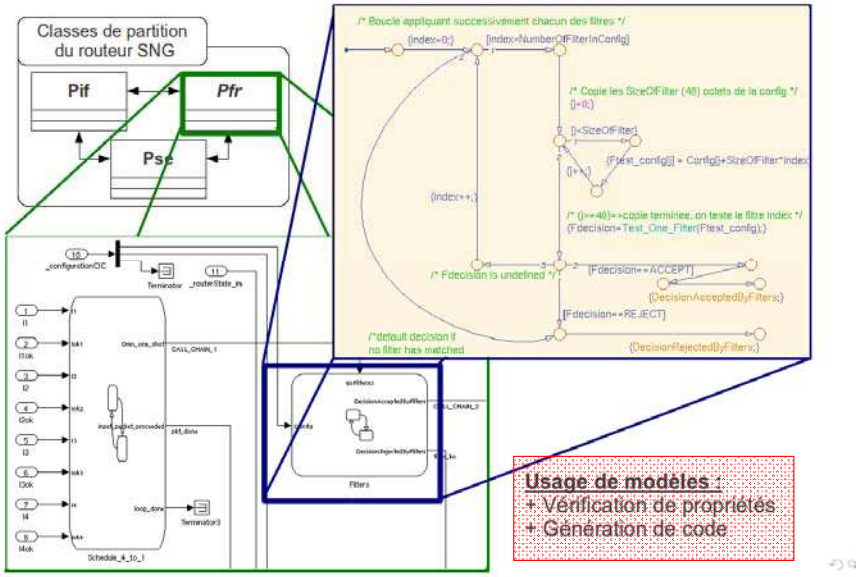
Très contraignant, ce qui nous a conduit à élaborer une méthodologie de développement rapide de logiciel qui tienne compte de l'évaluation et de la certification du logiciel produit.



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

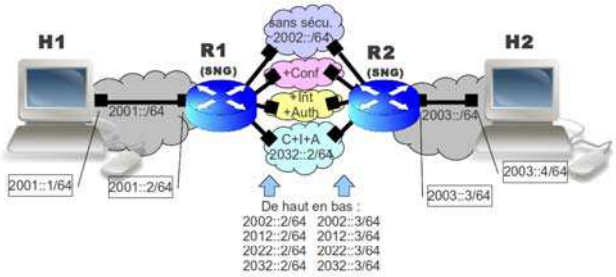
Le protocole *Internet Key Exchange version 2* (IKEv2 [rfc5996]) établit un chemin sécurisé appelé "canal" ou "tunnel" et négocie un jeu de clefs cryptographiques pour le protocole ESP.

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



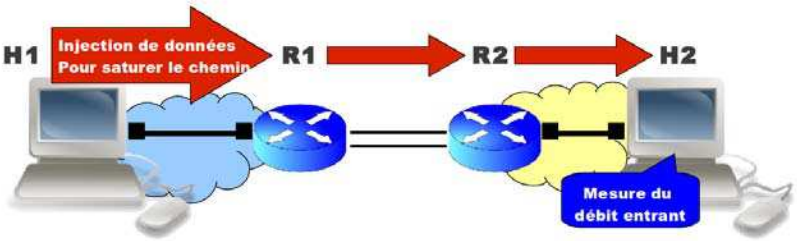
Permet de valider les classes de partition :

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

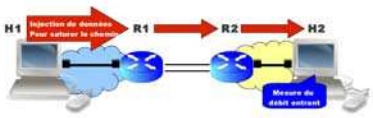
R1 et R2

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

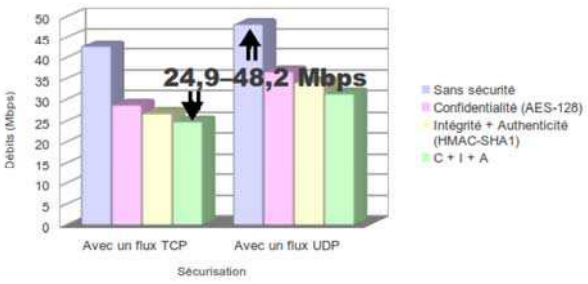
1/ Mesures de la capacité maximale du routeur SNG



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.

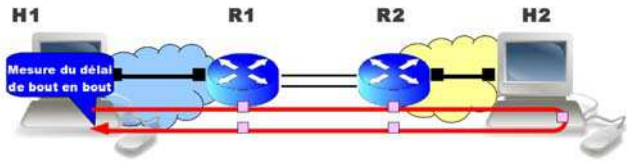
Modélisation de trafic de charge multiflux aéronautique

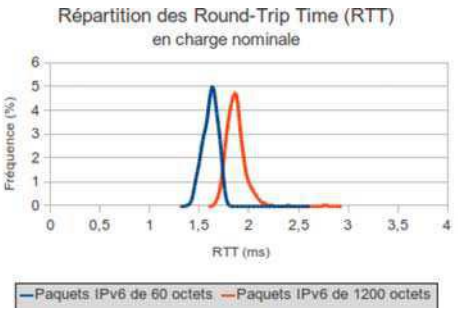
- Différents réseaux aéronautiques, différents besoins
- Trafic = ensemble de flux agrégés

Flux	Débits	Type de flux et profil
critiques	32.5 kbps	UDP, loi Uniforme *[cnes2009]*
non critiques (flux passagers"APC")	• ~500 kbps descendant • ~300 kbps montant *[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

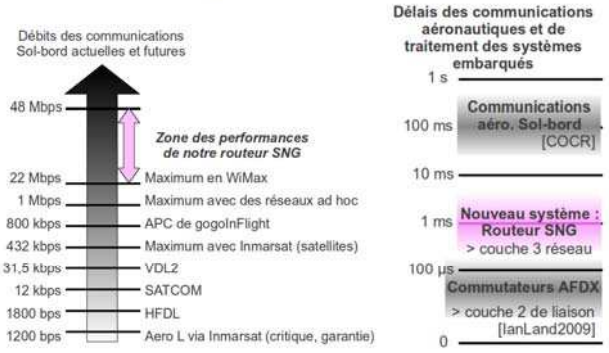
Modélisation de trafic de charge multiflux aéronautique

- 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

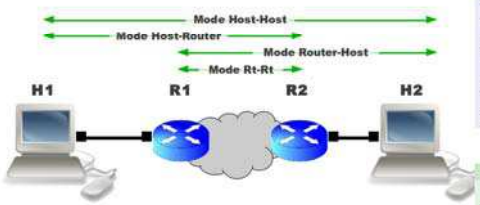
Répondeur

Le nœud qui décapsule les données sécurisées

Destinataire

Le nœud qui reçoit les données

Les 4 modes de fonctionnement de SCOUT

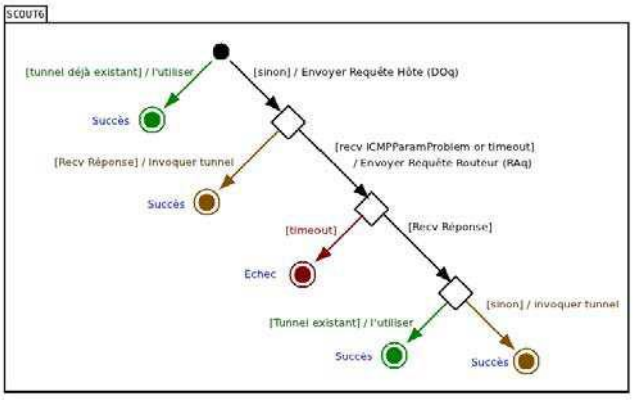


La sécurité dépend de la prise en charge de SCOUT sur les nœuds

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

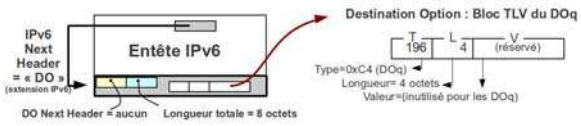
Le protocole SCOUT

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

Le protocole SCOUT6

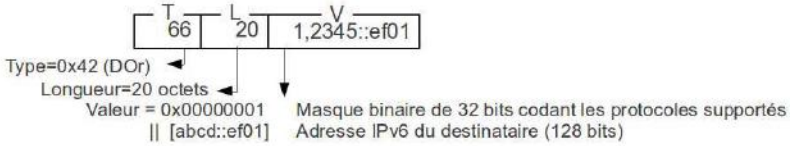
Instanciation de SCOUT avec les fonctionnalités introduites par le protocole IPv6

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

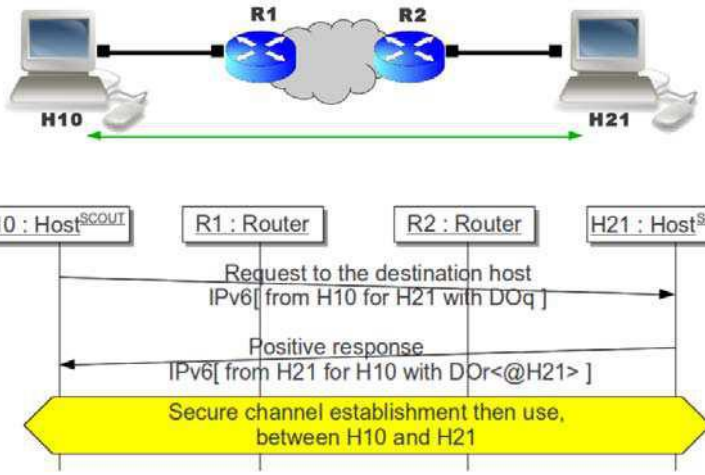
La requête routeur "RAq"

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

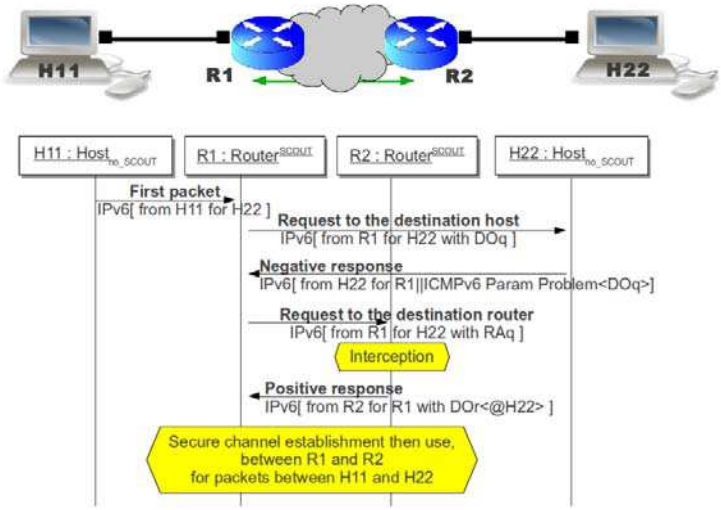
    les routeurs faisant suivre le paquet traitent l'option si elles savent le traiter, l'ignorent sinon

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

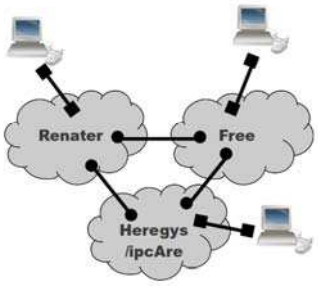
SCOUT6 en mode Host-host



SCOUT6 en mode Routeur-Routeur



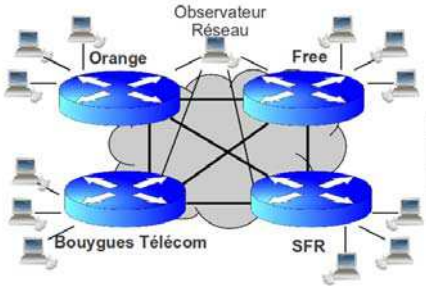
Validation sur Internet de SCOUT6



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

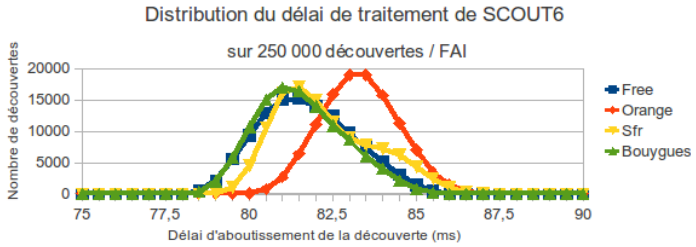


Délais moyens et gigue (en ms)

	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

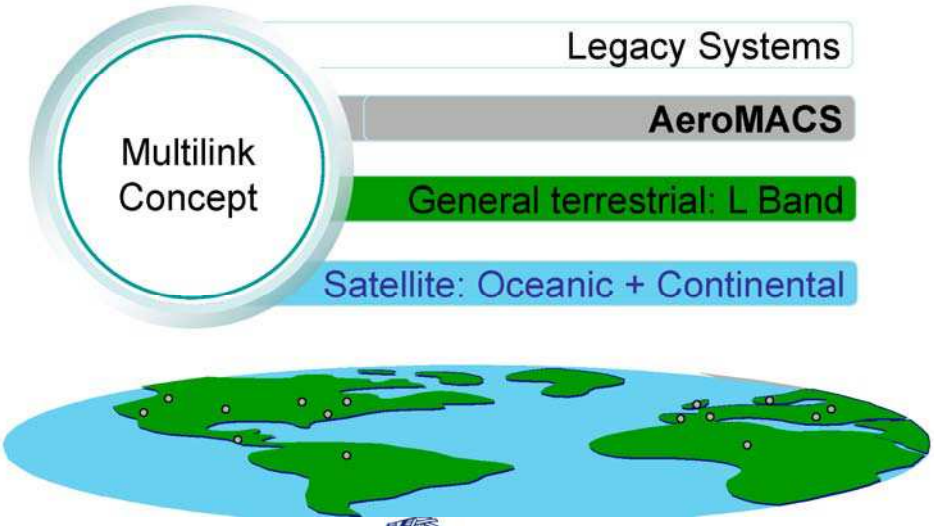
Future ATM concept requires **new ATM services**

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

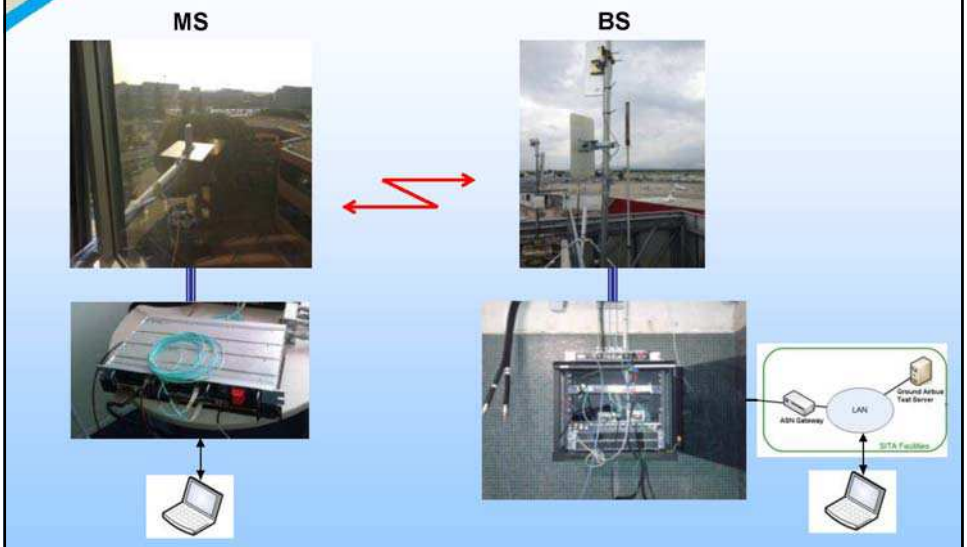
FOQA/FDR/ACMS related:
- Aircraft Telemetry Service
- Emergency Data Transfer
- FOQA Data Transfer
- …

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

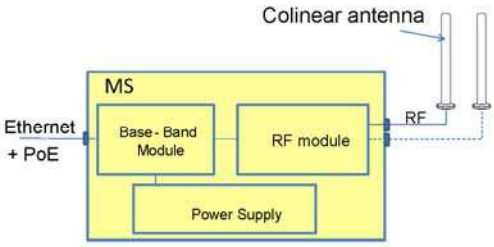
Toulouse Airport
AeroMACS MS/BS Installations



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

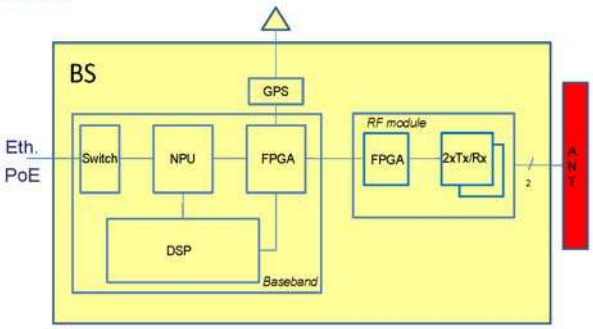
Viking S3-B

- 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



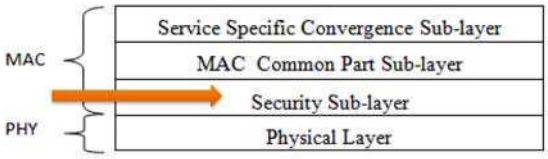
Dimensions: ~ 400 mm x 375 mm x 130 mm
Weight : ~ 12 Kg

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

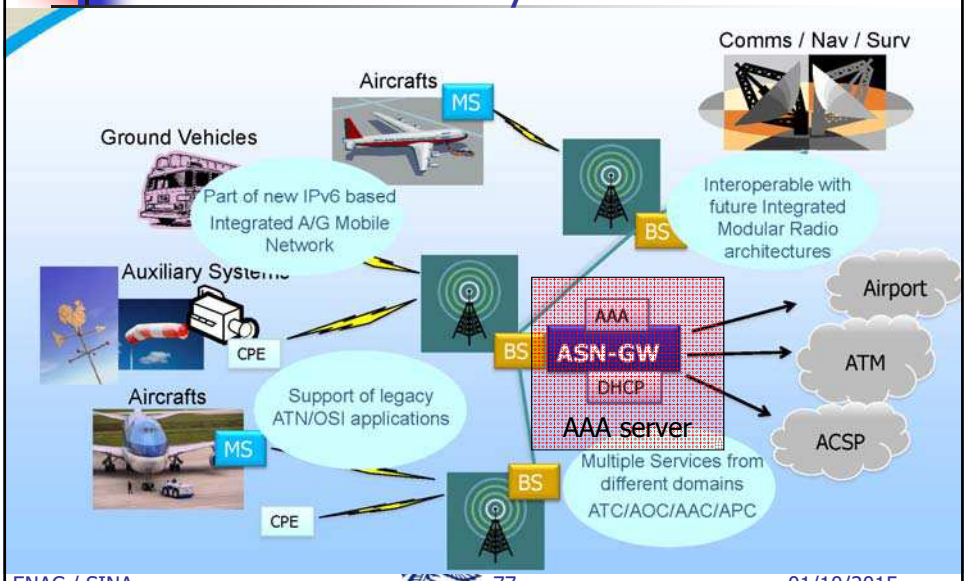


The WiMAX Security Sub-layer

A High-Level Features List – the Architecture:

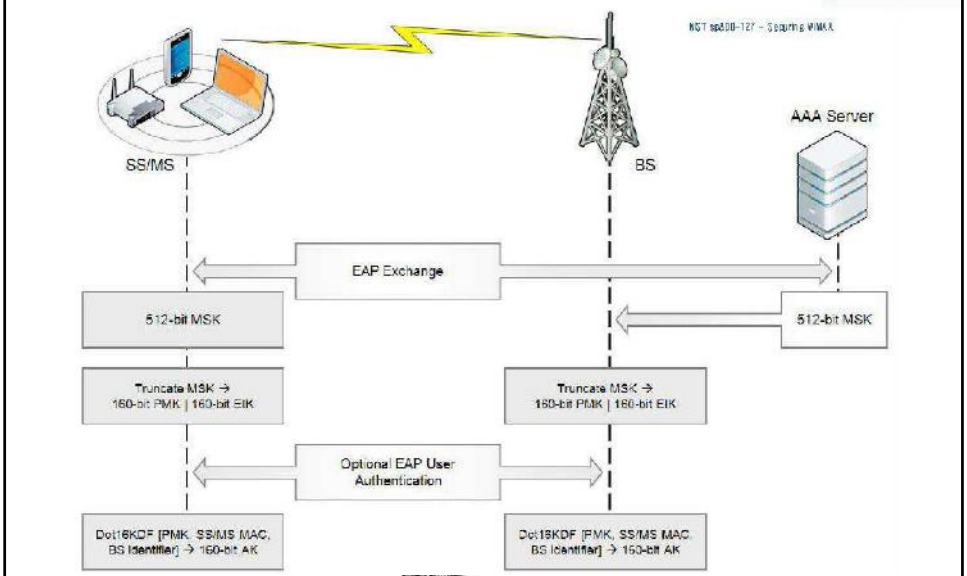
- Authorization Policy
- PKMv2 support
- EAP-based authorization
- CCM-mode with AES key-wrap
- Primary and static SA's
- Unicast SA (Multicast / Broadcast?)
- Encryption
- X.509

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

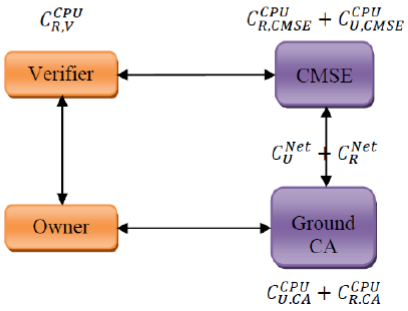
Performance-aware hierarchical PKI model for future aircrafts communications

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



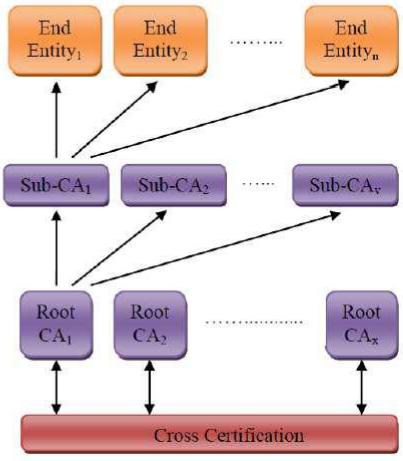
Hierarchical PKI model: design principles

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

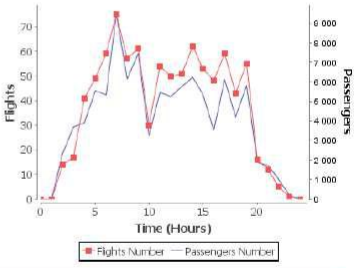
Extract (useful) data

- 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

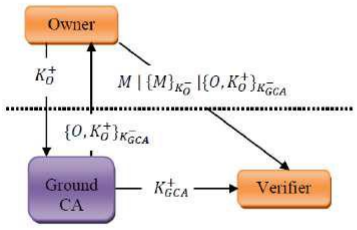
- RSA signature key length: 256 Bytes
- Certificate length: 1 KByte
- One certificate per user
- Exchanged data not considered
  ⇒ Only additional PKI signalling overhead is quantified here

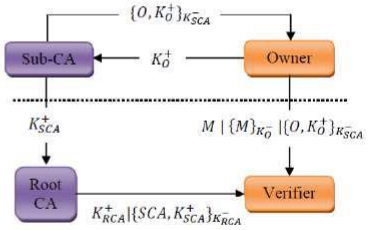
Acronyms and notations

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

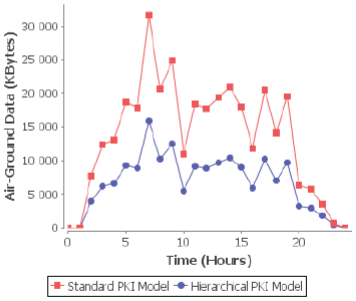
$N_f.l_{sig} + N_C.(l_{sig} + Size_C)$

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 %

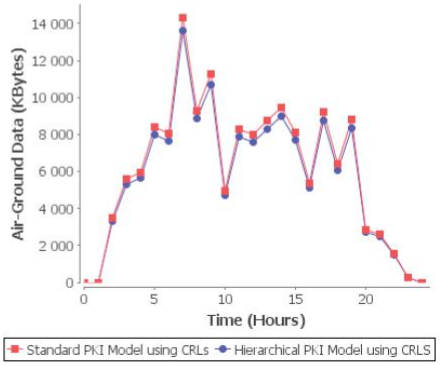
Costs for updating certificate revocation information

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



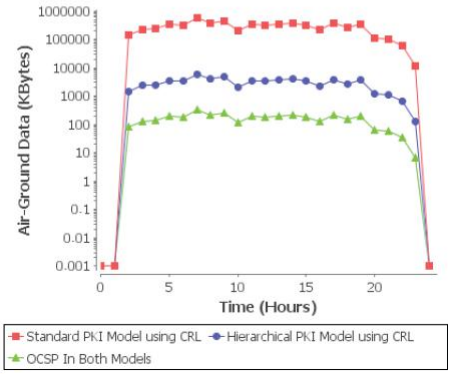
Costs for revocation requests

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**

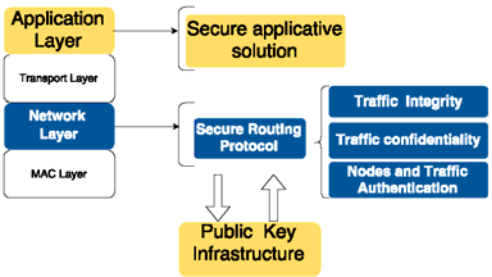
SUANET: secure UAANET

Thèse CIFRE: 2014-2017

delair-tech AIRBORNE SENSORING

SUANET research objectives

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



Plan

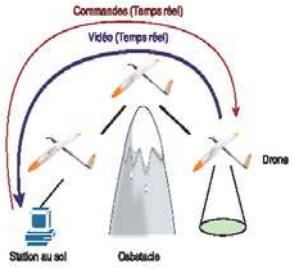
1. Introduction et contexte du travail
2. Élaboration d'une méthodologie de prototypage rapide
3. Création du protocole SUAP (Secure UAV Ad hoc routing Protocol)
4. Validation des performances du protocole SUAP
5. Conclusions & Perspectives

Drones civils

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

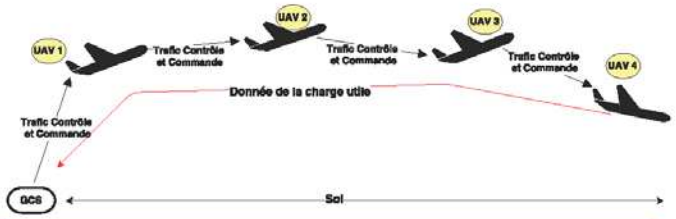
Drones civils

- **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

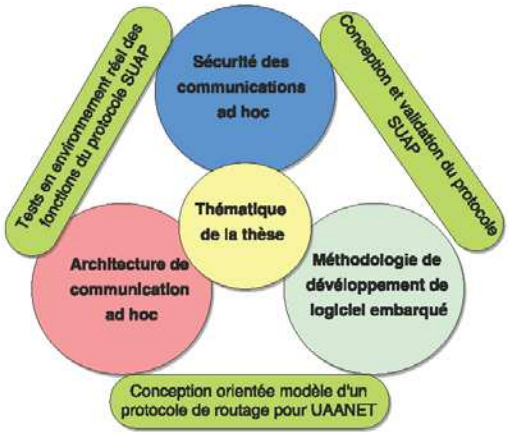
- Anticiper les défaillances et les pannes
- [DO 178 B], [DO 178 C] : normes de certification du logiciel pour l'avionique
- Vérification de conformité entre le code source et l'architecure logicielle durant la conception

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

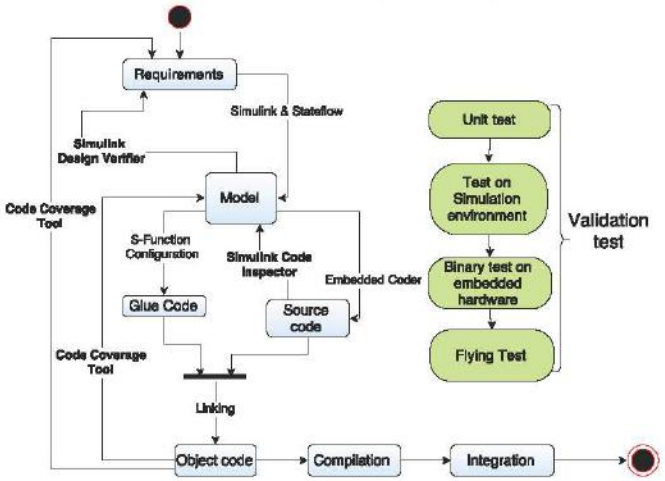
Contribuer à la validation (dans le but d'obtenir une certification) du système UAS utilisé

Domaines de recherche et contributions de la thèse



Plan

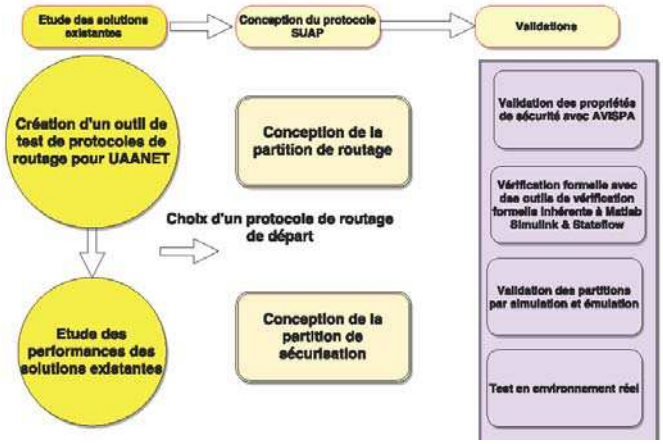
SUANET development process



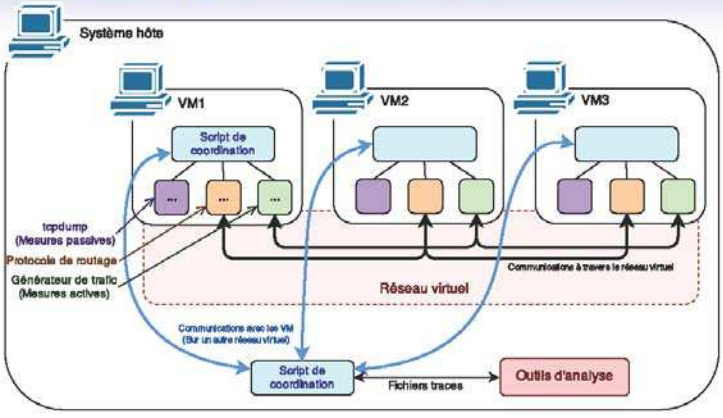
Plan

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

Processus de conception et de validation du protocole SUAP



Outil hybride d'évaluation pour UAANET



Etude des protocoles de routage existant

Cadre d'étude

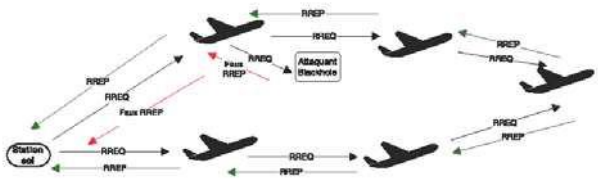
1. Modélisation d'environnement UAANET sous OMNET++
   - Développement d'un module de mobilité rejouant des trajectoires réelles
   - Execution des protocoles dans un système d'exploitation émulé (machine virtuelle VirtualBox)
   - Implémentation en C des algorithmes de routage utilisés
   - Génération 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)

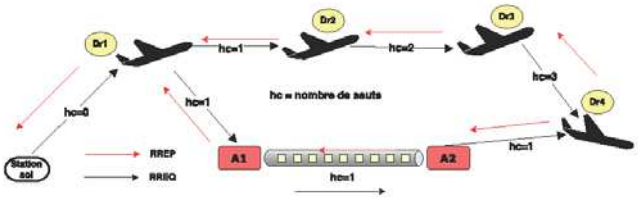
Mécanismes de sécurité des MANET existant

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

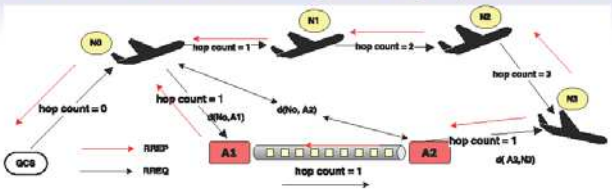
Authentification (des messages) entre voisin et vérification de l'existence d'un tunnel wormhole

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

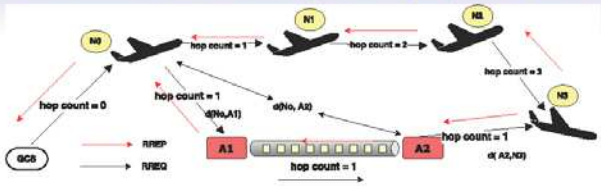
$$\frac{T}{Dmax} - 1 \leq hc < \frac{T}{Dmax} + 1 \quad (1)$$

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

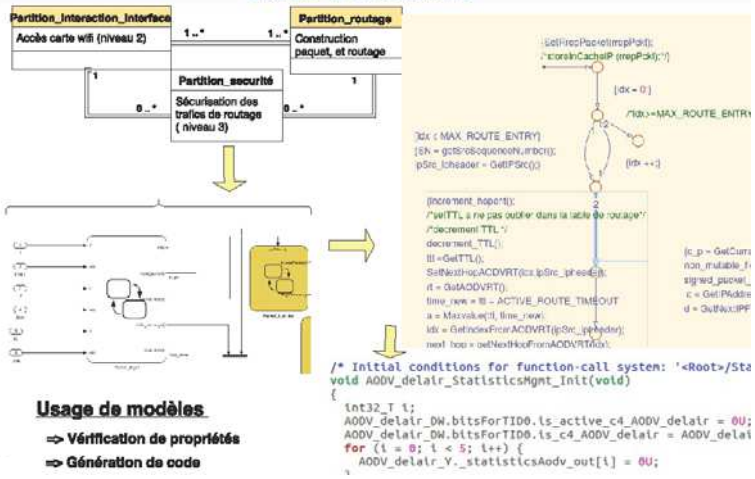
ETAPE 1 (à l'initialisation) : Découverte de voisin

- 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

```
/* Initial conditions for function-call system: '<Root>/Sta
void AODV_delair_StatisticsMgmt_Init(void)
{
  int32_T i;
  AODV_delair_DW.bitsForTID0.is_active_c4_AODV_delair = 0U;
  AODV_delair_DW.bitsForTID0.is_c4_AODV_delair = AODV_delai
  for (i = 0; i < 5; i++) {
    AODV_delair_Y._statisticsAodv_out[i] = 0U;
```


Plan

Validation des classes de partition

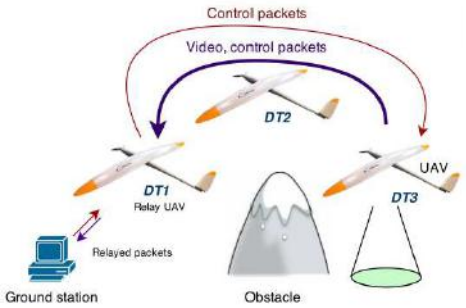
Test en environnement réel

- 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

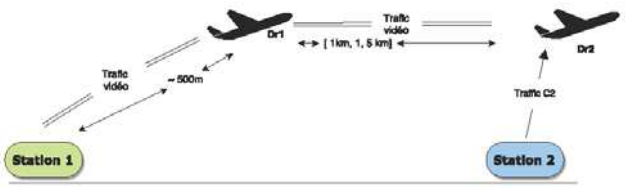
Flying testbed

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

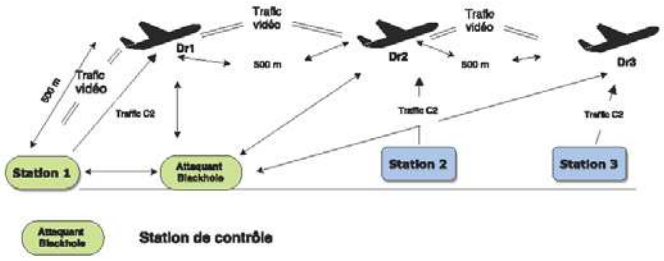
Résultats de performance de SUAP par rapport à AODV

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

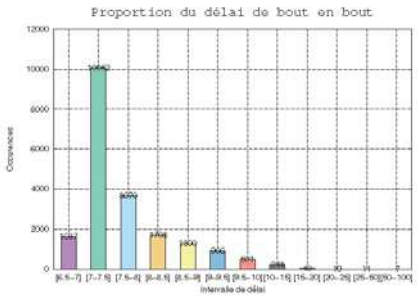


Permet de valider les classes de partition de sécurisation des trafics de routage

- 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

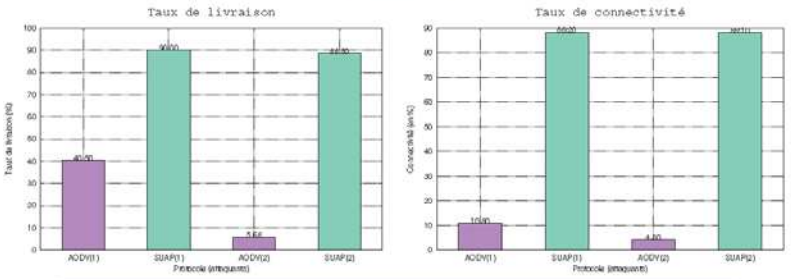


Délai pour trafic de signalisation	Valeurs
Délai moyen	7.43 ms
Délai maximum	100 ms
Délai pour trafic de charge utile	**Valeurs**
Délai moyen	9.2 ms
Délai maximum	104 ms

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



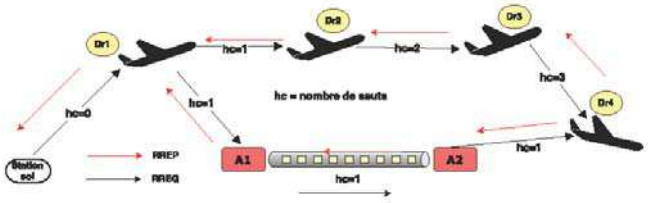
Conclusion

- 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

Formation : Sécurité des Communications Spatiales (COMSEC / TRANSEC)

Intervenant : W. HALIMI – THALES ALENIA SPACE

Presentation à l'ENSEEIHT - 09.01.2019

PLAN DE LA PRESENTATION

1. Missions et systèmes spatiaux cibles
2. Liaisons de données spatiales
3. Menaces applicables aux liaisons de données spatiales
4. Objectifs de sécurité résultants
5. Services de sécurité cibles
6. Algorithmes et modes d'opération cryptographiques
7. Gestion des Clés
8. Cas des systèmes COMSEC
9. Cas des systèmes TRANSEC
10. Conclusion, Discussion

1 - Missions et Systèmes Spatiaux Cibles

1.1 – Mission Spatiales : Type et Profil

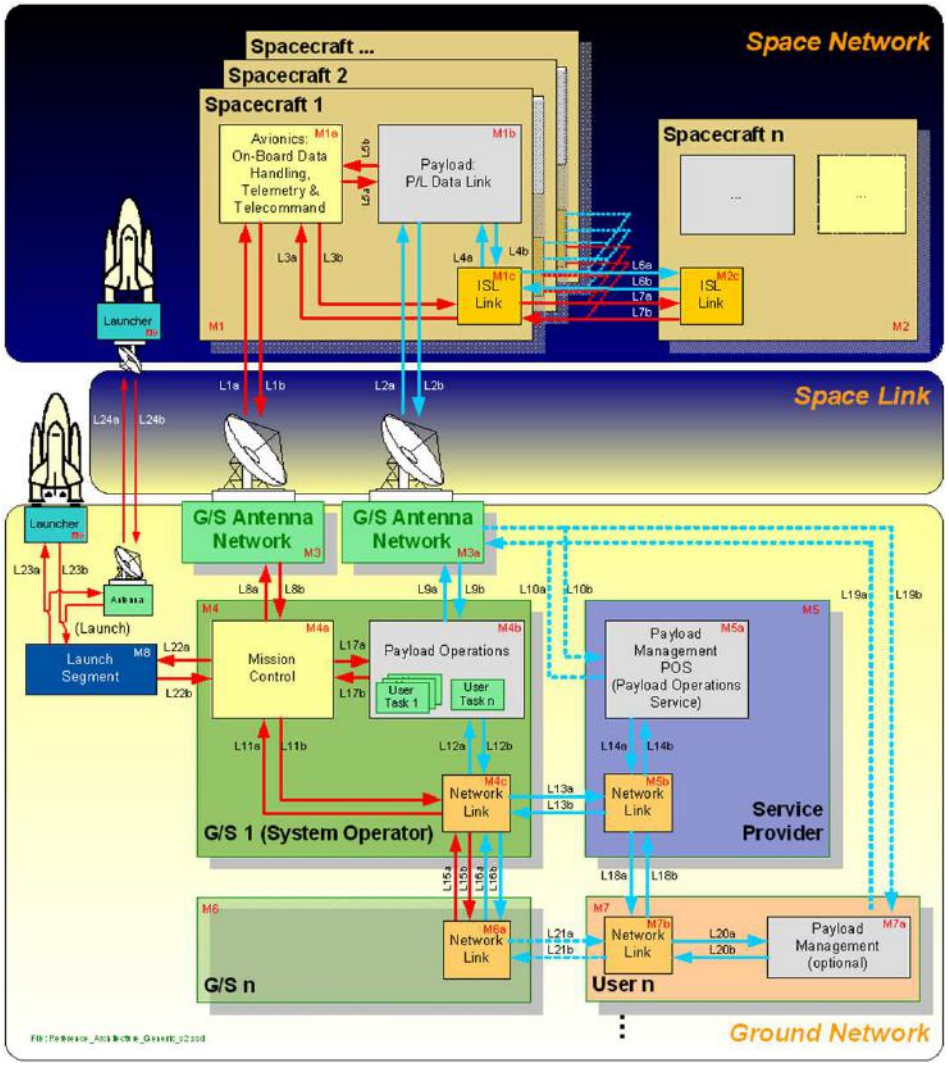
- Type de Mission
  - Télécommunication
  - Observation / Environnement / Sécurité civile
  - Scientifique
  - Navigation
- Profil Mission applicable à chaque type
  - Commerciale : ex EUTELSAT (TLC), SPOT (OBS)
  - Défense : Ex SYRACUSE (TLC)
  - Duale : Commerciale et Défense : ex PLEIADES (OBS), SGDC (TLC)

1.2 – Systèmes Spatiaux

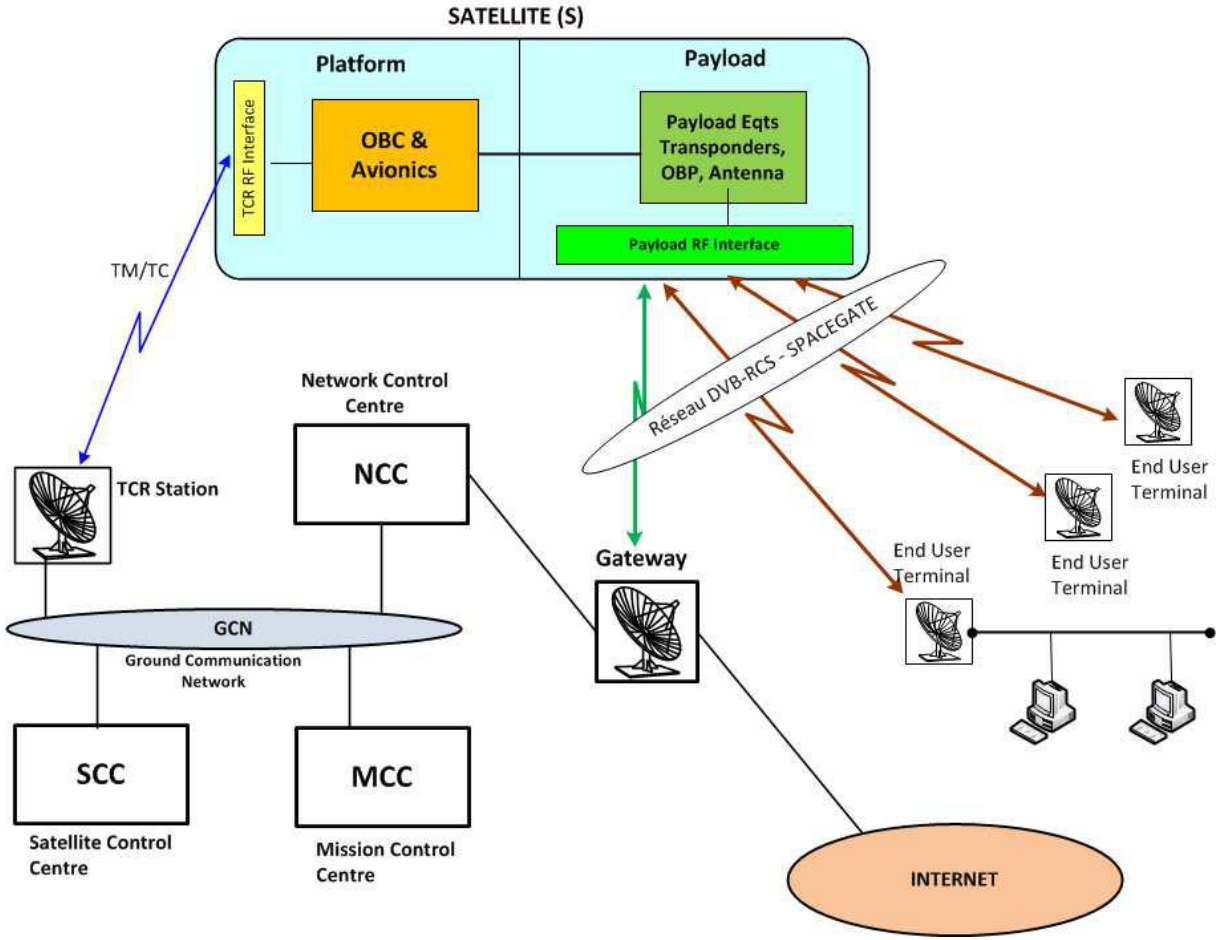
- Orbite
  - Géostationnaire : 36000 km
  - LEO (Low Earth Orbit) : orbite circulaire 500 à 2000 km
    - Période orbitale : environ 90 mn
  - MEO (Medium Earth Orbit) : 2000 à 30000 km
    - Ex: GLONASS, GPS, GALILEO
    - Période orbitale : 2 à 12h
- Configuration
  - Mono / Multi satellites
  - Constellation :
    - Telecom : IRIDIUM, O3B, GLOBALSTAR
    - Navigation : GPS, GALILEO, GLONASS
    - Avec ou non Liaison inter satellites (ISL) : exemple IRIDIUM-NEXT

1.3 – Configuration générale des systèmes spatiaux

- Segments Sol
  - Contrôle
  - Mission
  - Utilisateur
- Segment Spatial
  - Satellite(s)
- Segment Lanceur
  - Fusée Ariane5



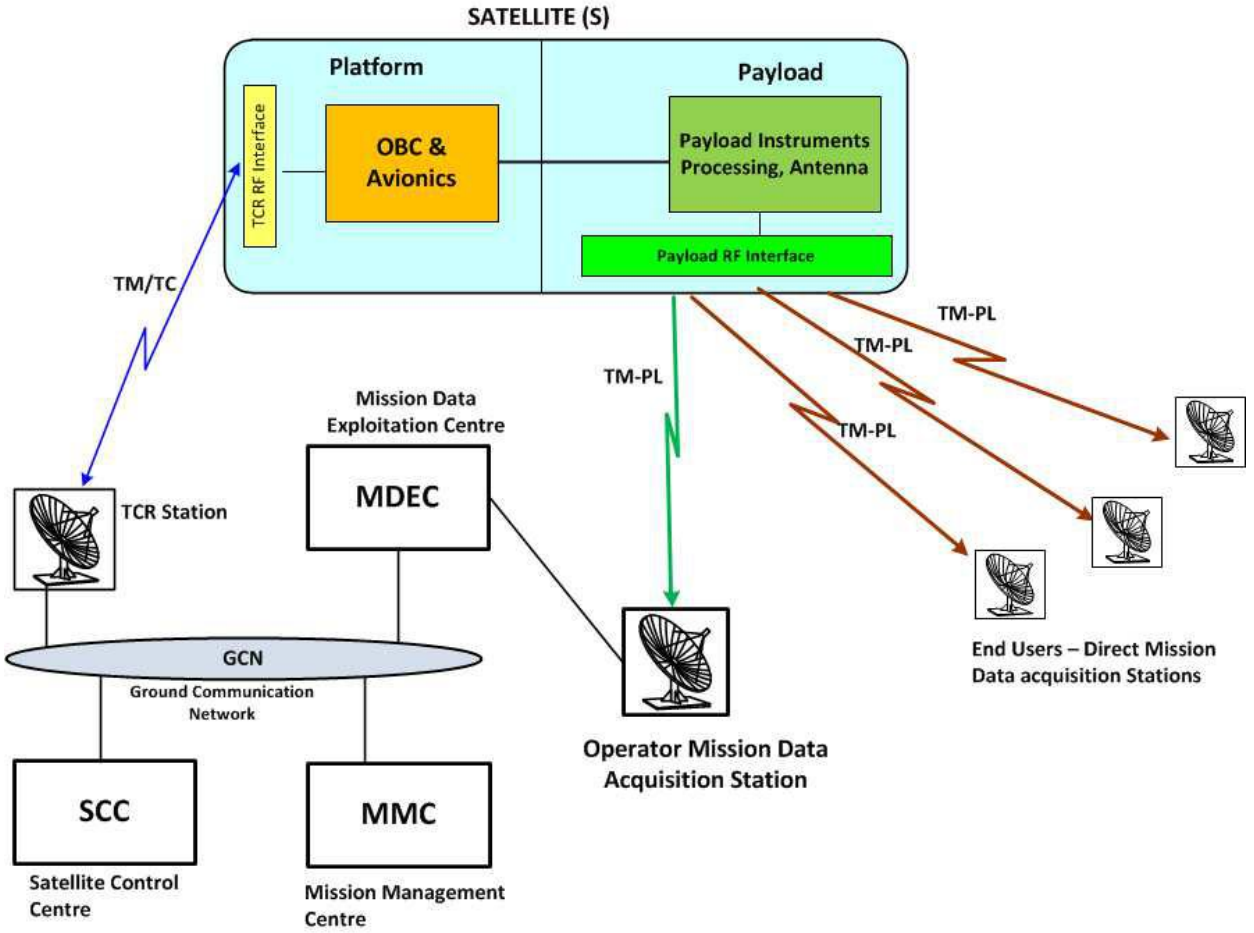
1.3 – Exemple : Mission Telecommunication (1/2)



1.3 – Exemple : Mission Telecommunication (2/2)

- SCC : en charge du contrôle et monitoring du satellite (maintien à poste)
- Station TCR (Telemetry Command Ranging) :
  - Assure l'interface Radio-Fréquence (RF) entre le SCC et le satellite
  - Gère les liaisons TC (Télécommande/montante), TM (Télémesure/descendante) et assure la fonction mesure de distance (Ranging) pour la localisation du satellite.
- MCC : gère la mission (Charge utile) du satellite
- NCC : gère le Segment Sol Utilisateur (SSU) et en particulier les Stations Gateways et ressources RF associées
- Terminaux : équipement des Utilisateurs finaux et assurant l'accès au service fourni par l'Opérateur satellite
  - Ex: Récepteur TV numérique / DVB, Accès à Internet via les Gateways ou Interconnexion de sites

1.3 – Exemple : Mission Observation / Image (1/2)



1.3 – Exemple : Mission Observation (2/2)

- SCC : en charge du contrôle et monitoring du satellite (maintien à poste)
- Station TCR (Telemetry Command Ranging) : idem Mission Telecom
  - Acces RF au satellite (liaison TM/TC) et ranging (localisation)
- MMC : assure la plannification de la Mission
  - Réception des démandes des Utilisateurs (ex: images / prises de vue)
  - Generation des plans de travail de la Charge utile du satellite (Instrument)
- MDEC : recoit les données instruments via la station d'acquisition dédiée de l'operateur, et génère les produits (ex: images) commandés par les Clients (acces indirect aux données Instruments bord)
- Stations d'acquisition des Utilisateurs : équipement des Utilisateurs finaux et assurant l'accès direct aux données instruments du satellite

2 – Définition des Liaisons de Données Spatiales

(Space Data Links)

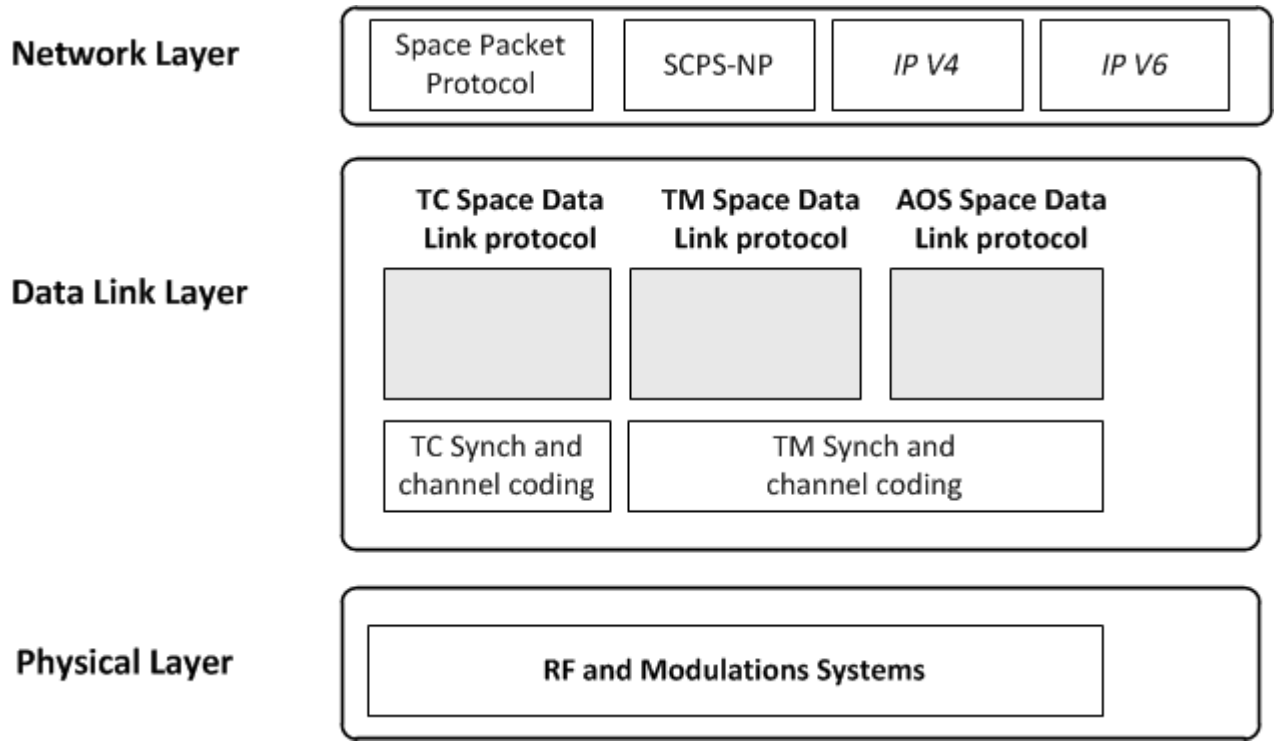
2.1 – Standard Space Data Links

Standards CCSDS

- CCSDS : Consultative Committee of Space Data Systems
  - Organisme regroupant toutes les agences spatiales et éditant les standards spatiaux
- TC Space Data Link Protocol : CCSDS 232.0-B-1
- TM Space Data Link Protocol : CCSDS 132.0-B-1
- AOS (Advanced Orbiting Systems) Space Data Link Protocol : CCSDS 732.0-B-2
- Space Data Link Security Protocol (SDLS) : 355.0-B-1
  - Standard Sécurité COMSEC pour data links TC / TM / AOS
  - Issue 1 sortie en Sept 2015

2.1 – Standard Space Data Links

Standards CCSDS : TC, TM, AOS => 3 couches



2.1 – Standard Space Data Links

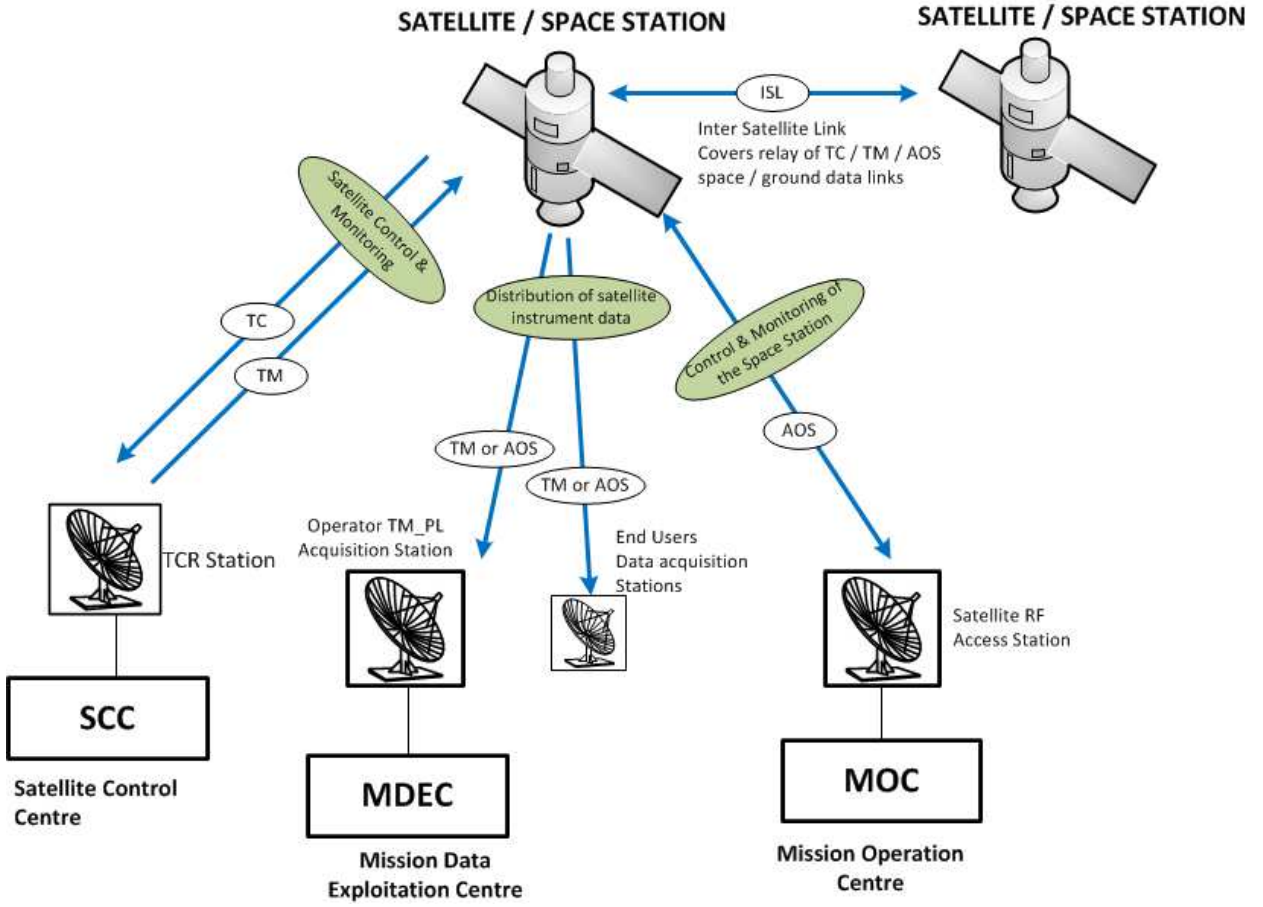
Standards ECSS : dérivés des standards CCSDS

- ECSS : European Cooperation for Space Standardization
  - Standards européens directement dérivés des standards CCSDS
  - Soutenu par l'ESA (Agence Spatiale Européenne) et les industriels européens
- Space data links – Telecommand protocols synchronization & channel coding - ECSS-E-ST-50-04C
- Space data links – Telemetry transfer frame protocol - ECSS-E-ST-50-03C

Standards ESA : dérivés des standards CCSDS

- Packet TC Standard : ESA-PSS-04-107
- Packet TM Standard : ESA-PSS-04-106
- Packet TC Decoder Specification : ESA-PSS-04-151
- Remplacés à terme par les standards ECSS

2.2 – Domaine d'application des Space Data Links (1/3)



2.2 – Domaine d'application des Space Data Links (2/3)

Standard TC (Télécommande)

- Liaison montante dédiée au contrôle du satellite
- Flux de données asynchrone et bas débit (< 100 kb/s)
- Associée à un protocole COP-1 assurant le séquencement et la retransmission des TC (Sequenced Controlled Service)

Standard TM (Télémesure)

- Liaison descendante
- Flux de données continu – liaison synchrone
- Utilisée pour le monitoring du satellite : Flux TM-HK (Télémesure de servitude)
  - Flux bas / moyen débit (< 100 kbs)
- Standard utilisé également pour le transport des données Instruments : Flux TM-PL pour les satellites Observation / Environnement / Scientifiques
  - Flux moyen débit jusqu'à très haut débit (1 Gb/s)

2.2 – Domaine d'application des Space Data Links (3/3)

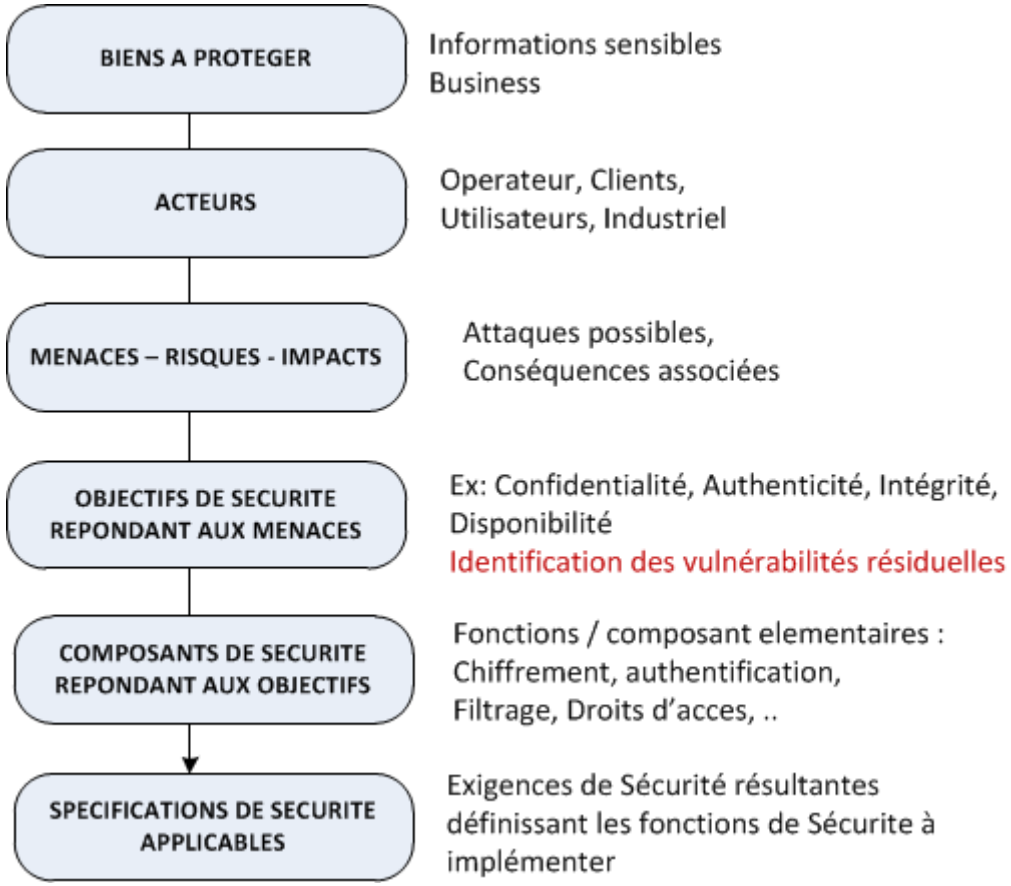
Standard AOS (Advanced Orbiting Systems)

- Couvre une liaison bidirectionnelle
- Flux multimedia : données, audio, video – liaison synchrone
- Utilisation multiple
  - Contrôle et monitoring d'une station spatiale (ex: station spatiale ISS)
  - Transport des données Instruments (liaison AOS seule) et alternative à la liaison TM pour le flux TM-PL
  - Echanges Audio / Vidéo avec équipage (ex: station spatiale ISS)

3 – Analyse de Risques & Menaces applicables aux Liaisons Spatiales

3 – Analyse de Risques et Menaces

- L'Analyse de Risque constitue la première étape de l'activité Sécurité (pour tout système)
- Différentes méthodologies existent et peuvent être appliquées dans le spatial
  - Critères Communs
  - NIST – Risks Analysis
  - EBIOS (ANSSI) : Identification des Besoins et Identification des Objectifs de Sécurité
- La logique d'analyse de risques illustrée ci-joint est issue de la méthodologie Critères Communs
- Sortie : Exigences de Sécurité applicables au système spatial à déployer



❑ Certification Sécurité : Critères Communs / NIST

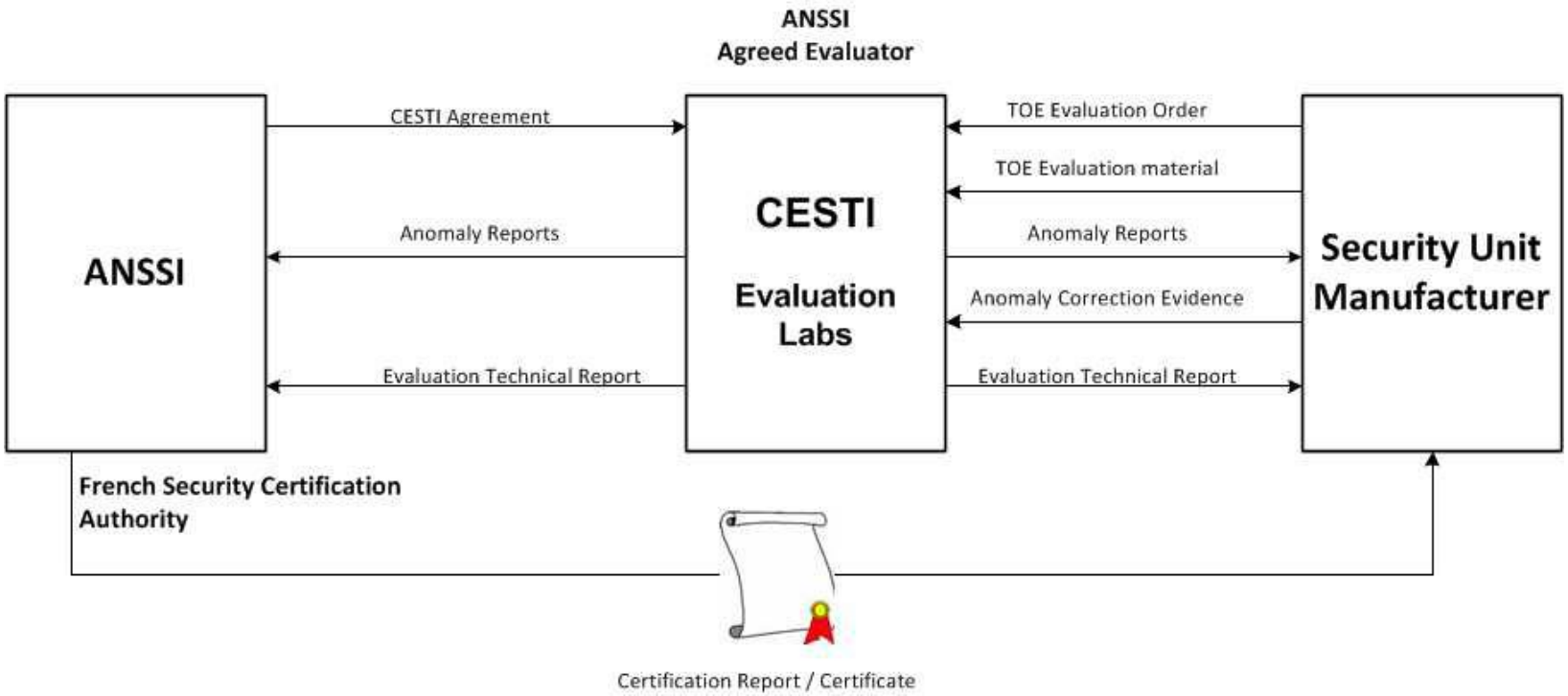
➢ Certification Critères Commun (CC)

- 7 niveaux d'Assurance Sécurité : EAL (Assurance Evaluation Level)
- Evaluation par un organisme agréé dit CESTI (en France agréé par ANSSI)
- Pour chaque équipement, l'évaluation se fait sur la base d'un document Cible de Sécurité (ST : Security Target) de la fonction cible (TOE : Target of Evaluation) incluant l'ensemble des exigences de sécurité à vérifier
- Inclut des tests de vulnérabilité poussés suivant le niveau EAL
- Certains tests de vulnérabilité (Classe AVA) peuvent être destructifs

➢ Certification NIST

- Basé sur les exigences définies dans le document NIST FIPS 140-3
- 4 niveaux d'assurance sécurité
- Evaluation par un organisme / laboratoire agréé par le NIST

❑ Certification Sécurité basée sur les Critères Communs (CC)



❑ Certification Critères Communs (CC): Cible de Sécurité (ST)

➢ ST = Spécification applicable d'entrée pour l'évaluation Sécurité par le CESTI

1 - Introduction
▪ Identification de la Cible de Sécurité
▪ Vue d'ensemble de la Cible de Sécurité
▪ Conformité aux CC
▪ Documents de référence
2 – Description de la TOE
▪ Présentation du système
▪ Présentation TOE
▪ Cycle de vie du produit
▪ Périmètre de la TOE
▪ Fonctionnalités de la TOE
3 – Environnement de la sécurité de la TOE
▪ Biens sensibles – classification
▪ Acteurs
▪ Typologie des attaquants
▪ Hypothèses (H)
▪ Menaces (M)
▪ Politique de sécurité organisationnelle (P)
4 – Objectifs de Sécurité
▪ Objectifs de sécurité pour la TOE (OT)
▪ Objectifs de sécurité pour l'environnement de la TOE (ONE)
▪ Tableau de correspondance Environnement / Objectifs : (H, M,P) ⇔ (OT,ONE)

5 – Composants de Sécurité
▪ Composants fonctionnels de sécurité pour la TOE - FAU, FCS, FDP, FMT, FPT, FTP
▪ *Exigences fonctionnelles associées*
▪ Composants fonctionnels de sécurité pour l'environnement de la TOE - FAU, FPT
▪ *Exigences fonctionnelles associées*
▪ Tableau de correspondance - OT ⇔ composants fonctionnels
▪ Composant d'Assurance de Sécurité ▪ Référence à EAL-4 + Annexe A
6 – Spécifications globales de la TOE
▪ Fonctions de sécurité - Identification de 11 SF
▪ Tableau de correspondance - SF ⇔ composants fonctionnels
▪ Identification des fonctions réalisées par des mécanismes stochastiques ou permutationnels
▪ Identification des fonctions réalisées par des mécanismes cryptographiques
▪ Déclaration du niveau de résistance
▪ Mesures d'assurance - MA1 à MA5
▪ Tableau de correspondance - Classe exigence assurance / mesures d'assurance - (ACM, ADO, ADV, AGD, ALC) ⇔ (MA1, .. MA5)

7 – Argumentaire
▪ Argumentaire de cohésion des composants
- composants fonctionnels de la TOE ▪ exigence – dépendances - argumentaire
- composants fonctionnels de l'environnement de la TOE ▪ exigence – dépendances - argumentaire
- composants d'assurance ▪ exigence – dépendances - argumentaire
Annexe A – Liste des exigences d'assurance de sécurité
▪ Classe ACM – Gestion de Configuration
▪ Classe ADO – Livraison et Exploitation
▪ Classe ADV - Développement
▪ Classe AGD – Guides
▪ Classe ALC – Support au Cycle de Vie
▪ Classe ATE - Tests
▪ Classe AVA – Estimation des Vulnérabilités

Principales Menaces sur l'interface Air (1/2)

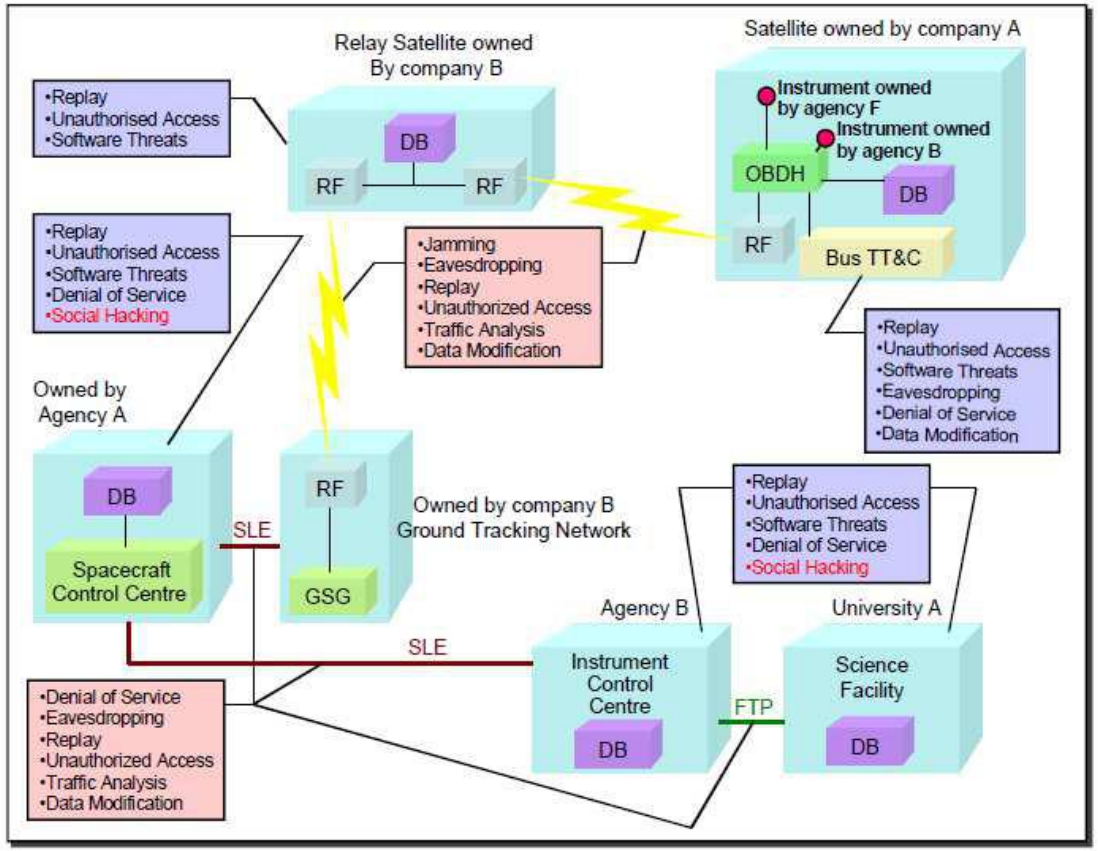
- Accès non autorisé à la fonction de commande (TC) du satellite
  - Intrusion active sur la liaison TC
  - L'intrus cherche à se faire passer pour le SCC et vise à transmettre des télécommandes au satellite
- Ecoute (Flux TC, TM-HK, TM-PL)
  - L'intrus écoute la ou les liaisons satellite : l'écoute passive est non contrôlable sur les liaisons RF bord / sol. Tout intrus équipé des moyens adéquats peut écouter
  - L'intrus prend connaissance des données / informations sensibles véhiculées sur ces liaisons
  - Idem avec les flux audio-vidéo véhiculés sur les liaisons AOS
- Rejeu (Flux TC)
  - L'intrus écoute la liaison TC et enregistre les commandes émises par le SCC authentique et qui sont donc valides
  - l'intrus re-émet ensuite ultérieurement les messages TC enregistrés au satellite en visant à ce qu'ils soient à nouveau acceptés par le satellite

Principales menaces sur l'interface Air (2/2)

- Modification intentionnelle des données (Flux TC, TM-HK, TM-PL)
  - Intrusion active sur la liaison montante ou descendante
  - Liaison montante Flux TC : L'intrus intercepte le message TC avant émission vers le satellite et modifie son contenu
  - Liaison descendante TM-HK, TM-PL : L'intrus intercepte le message TM avant acquisition par le SCC ou le Centre de traitement, et modifie son contenu
- Analyse de Trafic
  - L'intrus écoute et enregistre la ou les liaisons satellite (écoute passive)
  - En analysant le contenu des messages enregistrés (header, identifiants, adresses), il peut déterminer qui est l'émetteur (ex: quel satellite ou quel SCC) et le destinataire (ex: équipement / application dans le satellite)
  - Champs concernés : SCID, VCID, MAPID, APID, PUS Service ID , @ bus 1553
- Brouillage RF (Flux TC)
  - L'intrus utilise un brouilleur RF suffisamment puissant pour rendre la liaison TC inopérante (le SCC n'arrive alors plus à transmettre de TC acceptée par le satellite)
  - Menace de type **DoS** (Denial of Service) contre la disponibilité de la liaison TC

Principales Menaces (reference CCSDS)

- Document CCSDS 350.1-G-1 : Security Threats against Space Missions



3.3 – Cyber Securité & Systèmes Spatiaux

- Le développement très important des attaques au sol contre les systèmes d'information utilisant des réseaux de communication divers (Internet, réseaux mobiles, ..), a conduit durant la derniere decennie à développer le concept nouveau de Cyber-Securité destiné à adresser toutes les menaces et contre-mesures associées, ainsi que la détection / supervision des systèmes à implémenter

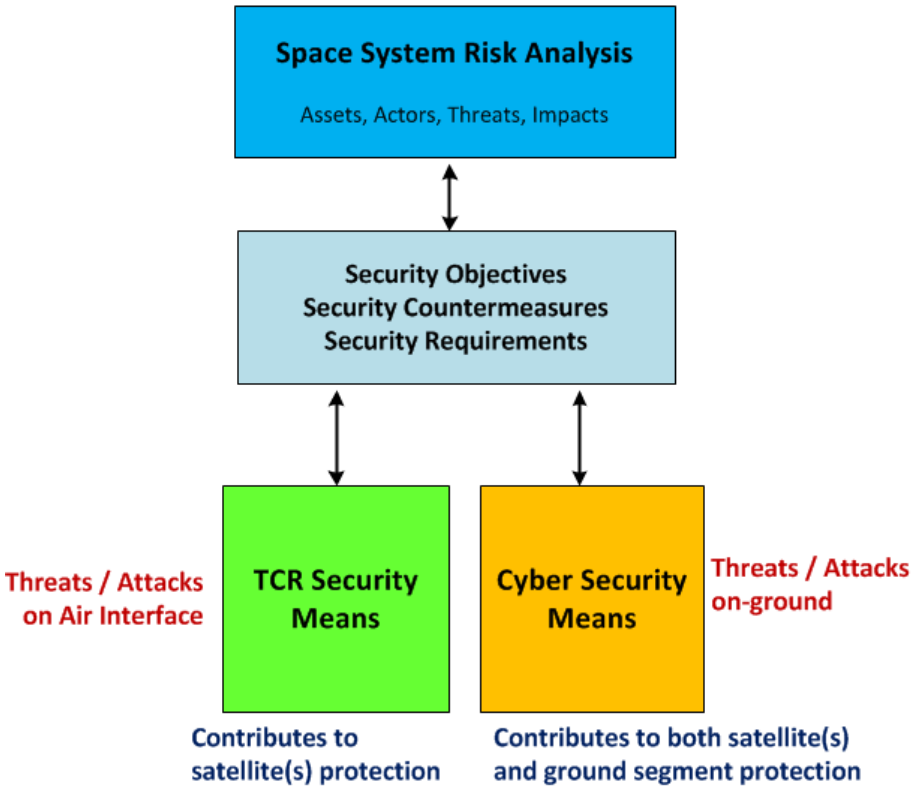
- USA / NSA : Executive order 13636 (2013) :
  - Improving Critical Infrastructure Cybersecurity - Preliminary CyberSecurity framework- Energy, Transport, Telecommunication, Finance

- NIST
  - NIST framework for improving critical infrastructure cybersecurity [2014]
  - NIST roadmap for improving critical infrastructure cybersecurity [2014]

- EU : Network and Information Security Directive of the 7th February 2013

- Autres initiatives : NATO, ENISA, National (BSI, ANSSI, ..)

Rôles distincts et complémentaires de la Cyber Sécurité et de la Sécurité TCR (Sécurite bord / sol) dans un système spatial



4 – Objectifs de Sécurité Résultants

Liaison TC / Flux TC (Commande du Satellite)

- Authenticité de la source
  - Le satellite ne doit accepter des TCs que si l'authenticité de la source (SCC de l'operateur) est vérifiée
- Intégrité des messages
  - Le satellite ne doit accepter des TCs que si leur intégrité (aucune modification intentionnelle ou non du message source) est vérifiée
- Anti-rejeu
  - Le satellite doit rejeter toute TC déjà transmise antérieurement
- Confidentialité des messages
  - Les données contenues dans un message TC ne doivent être accessibles qu'au satellite cible de l'opérateur
- Disponibilité
  - La liaison TC doit rester disponible (avec si besoin des performances réduites) même en cas d'attaque de type brouillage / DoS

Liaison TM / Flux TM-HK (Télémesure de Servitude)

- Authenticité de la source
  - Le SCC ne doit accepter des messages TM que si l'authenticité de la source (satellite de l'operateur) est vérifiée
- Intégrité
  - Le SCC ne doit accepter des messages TM du satellite que si l'intégrité (aucune modification intentionnelle ou non du message source) est vérifiée
- Confidentialité
  - Les données contenues dans un message TM ne doivent être accessibles qu'au SCC de l'opérateur satellite

Remarque

- Pour les liaisons TC comme TM, l'objectif de Non Répudiation n'est pas retenu comme besoin réel, l'authenticité de la source étant considérée comme suffisant
- Ceci permet notamment pour la protection du Trafic TC / TM de s'affranchir du besoin de **signature électronique** réquérant l'utilisation de la cryptographie asymétrique (ex: DSA, RSA-PSS, ECDSA)

Liaison TM / Flux TM-HK (Télémesure de Servitude)

- Authenticité de la source
  - Le SCC ne doit accepter des messages TM que si l'authenticité de la source (satellite de l'operateur) est vérifiée
- Intégrité
  - Le SCC ne doit accepter des messages TM du satellite que si l'intégrité (aucune modification intentionnelle ou non du message source) est vérifiée
- Confidentialité
  - Les données contenues dans un message TM ne doivent être accessibles qu'au SCC de l'opérateur satellite

Remarque

- Pour les liaisons TC comme TM, l'objectif de Non Répudiation n'est pas retenu comme besoin réel, l'authenticité de la source étant considérée comme suffisant
- Ceci permet notamment pour la protection du Trafic TC / TM de s'affranchir du besoin de **signature électronique** requérant l'utilisation de la cryptographie asymétrique (ex: DSA, RSA-PSS, ECDSA)

5 – Services de Sécurité Cibles

La protection des liaisons de données spatiales TM/TC/AOS couvre deux familles de services de sécurité

- Service de Securite de type COMSEC (COMmunication SECurity)
  - Implémenté au niveau de la couche Liaison de Données (Data Link) du modèle en couches CCSDS
  - Opère sur les messages numériques transportés sur les liaisons TC/TM/AOS et traitées par la couche Data Link
  - Couvre les Services Authentification et Chiffrement
  - **Authentification** : répond aux objectifs => Authenticite , Intégrite, Anti-rejeu,
  - **Chiffrement** : répond à l'objectif => Confidentialité

- Service de Sécurité de type TRANSEC (TRANsmission SECurity)
  - Implémenté au niveau de la couche Physique Radio-Fréquence (Physical Link) du modèle en couches CCSDS
  - Répond à l''objectif de Disponibilité
    - protection contre le brouillage RF / menaces de type DoS (Denial of Service)
    - A pour objet de garantir la disponibilité de la liaison TC sous certaines conditions dégradées

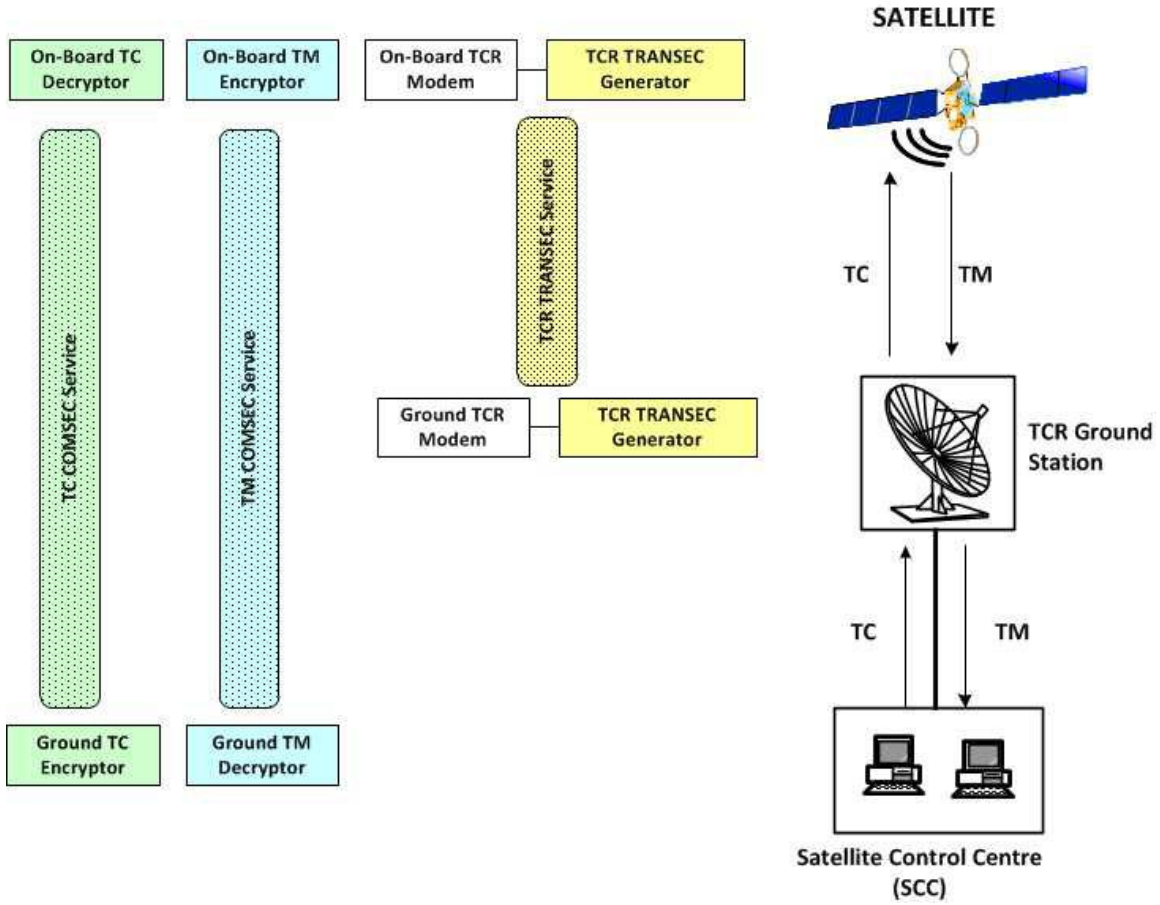
Services de Sécurité applicable aux liaisons de données spatiales

- TC-COMSEC-1 - (Flux : TC)
  - Service de sécurité implémenté : Authentification (AO : Authentication Only)
    - Protection : Authenticité , Intégrité, Anti-rejeu
    - Pas de besoin de confidentialité (missions commerciales / scientifiques)
- TC-COMSEC-2 (Flux : TC)
  - Services de Sécurité implémentés : Authentification + Chiffrement (AE : Authenticated Encryption)
    - Protection : Authenticité , Intégrité, Anti-rejeu , Confidentialité
- Note : Le service Authentification est obligatoire en TC (service minimal)
- TC TRANSEC (Flux : TC)
  - Services de Sécurité implémenté : Anti-brouillage

Services de Sécurité applicable aux liaisons de données spatiales

- TM COMSEC (Flux : TM-HK ou TM-PL)
  - Services de Sécurité implémentés : Authentification + Chiffrement (AE : Authenticated Encryption)
    - Protection : Authenticité , Intégrité, Confidentialité
- AOS COMSEC (Flux AOS Audio-Vidéo)
  - Service de Sécurité implémenté : Chiffrement (EO : Encryption Only)

Exemple de localisation des fonctions de Sécurité COMSEC & TRANSEC



6 – Algorithmes Cryptographiques Candidats

Modes d'Opération et Primitives

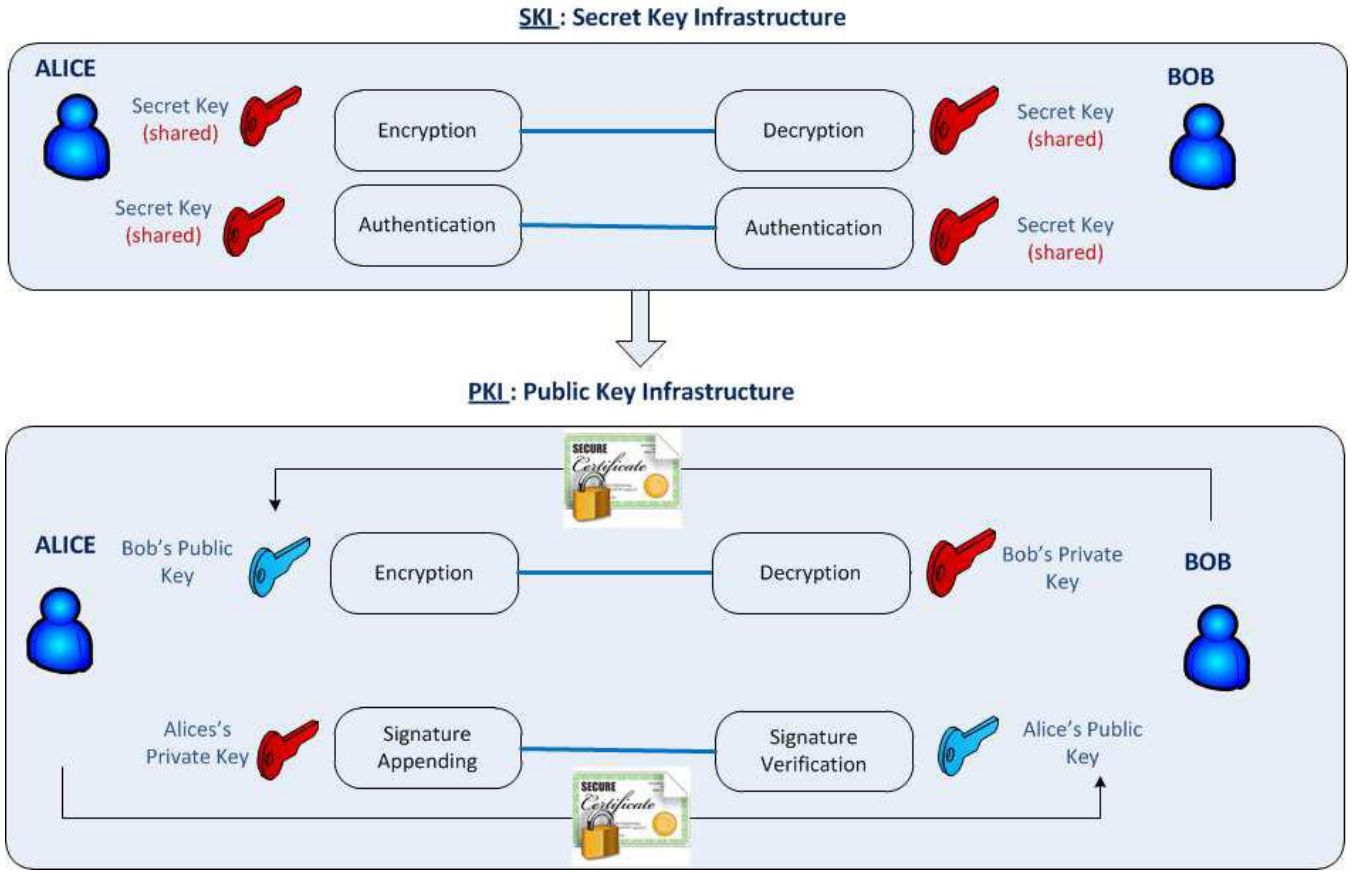
Techniques actuelles utilisées en cryptographie

- Cryptographie **symétrique** basée sur le partage préalable de clés secrètes entre les 2 utilisateurs communiquant
  - SKI : Secret Key Infrastructure
- Cryptographie **asymétrique** basée sur l'allocation d'un couple de clés Privée / Publique (PRK/PBK) à chaque utilisateur et sans aucun partage préalable d'éléments secrets
  - PKI : Public Key Infrastructure
  - La PRK est la propriété exclusive d'un acteur unique (pas de partage)
  - La PBK est diffusée via un certificat la liant formellement à son propriétaire
    - Certificat : PBK + User ID + Aux data => signée par une Autorité de Certification (CA)

Techniques émergentes en cryptographie

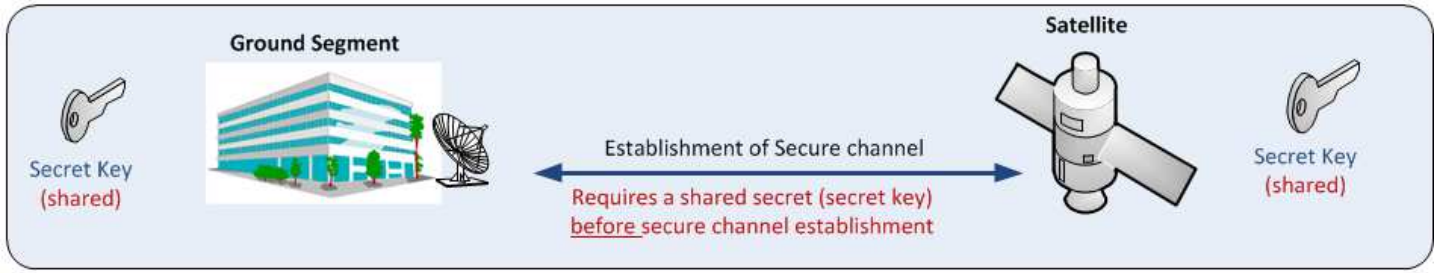
- Cryptographie post-quantique : algorithmes PKI résistant aux ordinateurs quantiques
- Cryptographie quantique / QKD (Quantum Key Distribution) : utilisation de liaisons optiques quantiques pour distribuer des clés de manière inviolable

Cryptographie Symétrique (SKI) vs Cryptographie Asymmétrique (PKI)

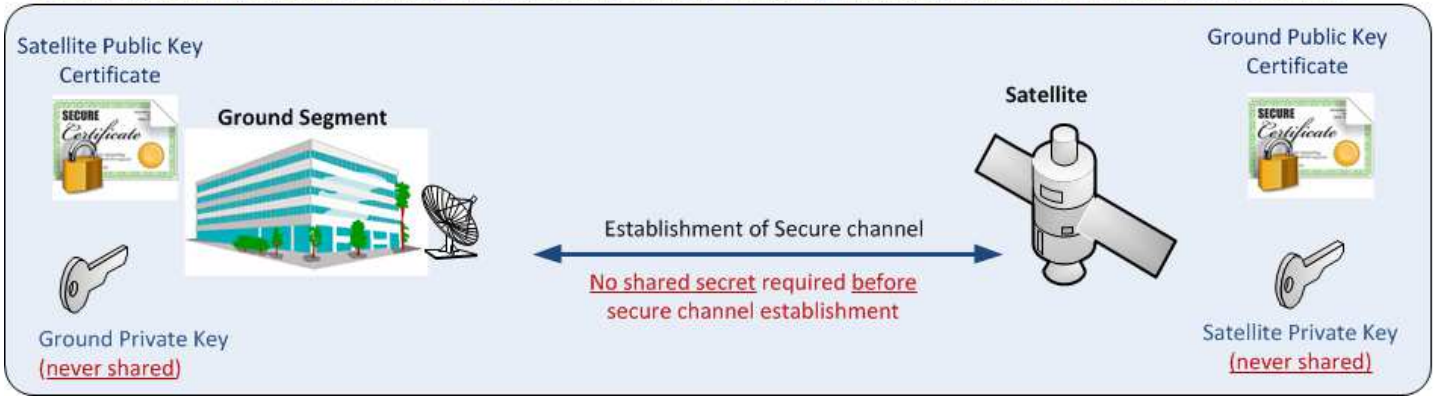


Cryptographie Symétrique (SKI) vs Cryptographie Asymétrique (PKI)

SKI : Satellite & Ground must shared a secret key before any establishment of a secure channel
Secret Key cannot be bound to a unique / exclusive owner (known by at least two entities)

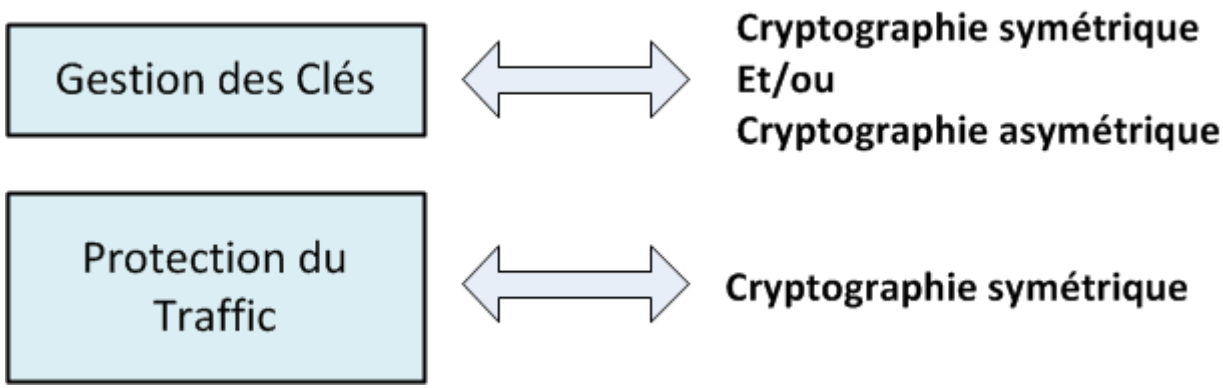


PKI : Satellite & Ground do not share any secret key before establishment of a secure channel
Public Key can be bound to identity of an exclusive owner (Ground or Satellite) via use of a Public Key Certificate



Utilisation de la SKI vs PKI dans le spatial

- La protection du Trafic bord / Sol TC, TM, AOS (services COMSEC / TRANSEC) n'utilise que la cryptographie symétrique
  - Le standard CCSDS Space Data Link Security (CCSDS 355.0-B-1) ne retient que l'utilisation de la cryptographie symétrique pour la protection COMSEC du trafic TC / TM
  - Aucun besoin de sécurité imposant la cryptographie PKI (ex: Non Répudiation)
- La Gestion des clés
  - Utilise encore largement la cryptographie symétrique
  - Evolue vers la cryptographie asymétrique



Cryptographie Symétrique (SKI)

- Avantages de la Cryptographie Symétrique pour la protection du Trafic
  - Algorithmes et modes d'opération parfaitement connus et maîtrisés
  - Implémentation aisée et optimisée: logicielle, matérielle (FPGA / ASIC)
  - Solutions peu gourmandes en ressources bord / satellite (CPU, mémoire, ..)
  - Performances très élevées en débit (protection du trafic) : compatibles de débits allant jusqu'à 1 Gb/s pour les données Instruments (Flux TM-PL)
  - Performances très honorables au niveau implémentation logicielle avec l'AES
- Un Algorithme cryptographique est composé:
  - D'un Mode d'opération (ex: GCM, CTR, CBC, CMAC, HMAC, ..)
  - D'une ou plusieurs primitives cryptographiques (ex: AES, SHA-128/256/384)

Sélection des Modes d'opération : Critères (1 / 2)

- Type : AO (Authentication Only), EO (Encryption Only, AE (Authenticated Encryption)
- Standardisation : NIST, RFC/ IETF, ISO
- Niveau de déploiement / adoption par l'industrie (spatiale ou non)
- Soumis ou non à Brevet (ex: RSA, OCB, PMAC)
- Sécurité vérifiable / démontrable (existence preuve de sécurité)
- Niveau de Sécurité : IND-CPA, IND-CCA, NM-CPA, INT-CTXT, INT-PTXT
- Choix des Primitives Cryptographiques utilisables : Hash / SHA-xxx, Block cipher AES (NIST FIPS 197) ou autres block cipher (ex: CAMELLIA, SEED)
- Tailles des clés
- Nombre de clés utilisées : distinction clés Chiffrement et Authentification
  - exigence RGS ANSSI
- Contrainte sur la taille max des messages

Sélection des Modes d'opération : Critères (2/2)

- Taille max du MAC / incrémentalité: niveau de Sécurité et overhead Sécurité
- Contraintes relatives aux Counter/IV/Nonce : Unicité, non déterminisme
- Propagation d'erreur
- Auto-synchronisation
- Padding / Expansion du ciphertext : impact sur overhead sécurité
- Nombre d'invocations des primitives cryptographiques pour chaque opération
  - Impact sur les performances
- Capacité de Preprocessing
  - Ex: pré-calcul des clés dérivées
- On-line – Off-line (ex: GCM vs CCM): impact sur les performances
- Parallelisation du traitement : impact sur les performances
- Performances implémentations matérielles / logicielles (Benchmark)

Mode d'Opération de type AO (Authentication Only)

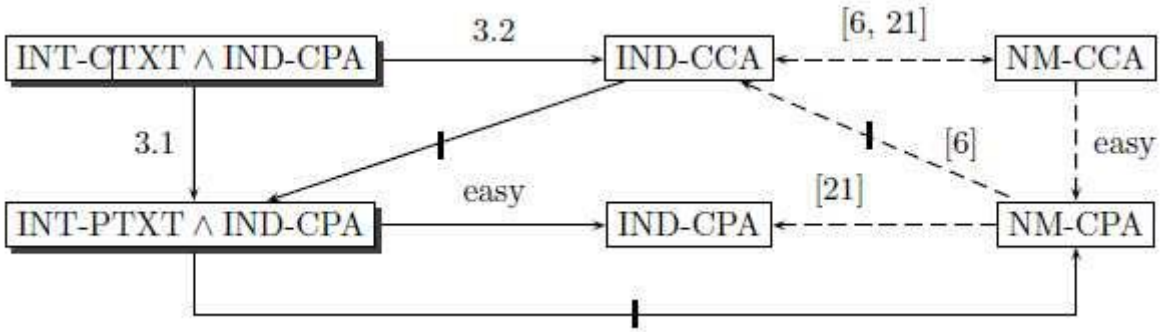
- Utilisation typique : service TC COMSEC lorsqu'il n'y a pas de besoin de confidentialité
  - Ex: Missions purement
  - Commerciales ou scientifiques

Scheme	Classification		Building Block
	Legacy	Future	
CMAC	✓	✓	Any block cipher as a PRP
HMAC	✓	✓	Any hash function as a PRF
UMAC	✓	✓	An internal universal hash function
EMAC	✓	✗	Any block cipher as a PRP
GMAC	✓	✗	Finite field operations
AMAC	✓	✗	Any block cipher

- Modes d'Opération candidats
  - CMAC : NIST SP800-38B
    - Corrige les vulnérabilités
    - du mode initial CBC-MAC
  - HMAC : NIST FIPS 198a
  - UMAC : utilise les fonction Hash Universal-2 de Wegman-Carter
- Remarques
  - PMAC (Parrallelizable MAC) de J. Black / P. Rogaway – encore soumis à brevet – non retenu
  - Le mode AO GMAC (NIST SP800-38D) non retenu dû à ses défauts & faiblesses
    - impose l'utilisation d'un IV contrairement aux autres modes AO / MAC
    - impact en cas de collision d'IV => compromission possible de la Clé GHASH

Mode d'Opération de type AE (Authenticated Encryption)

- Utilisation typique : service TC COMSEC (lorsqu'il y a besoin de Confidentialité) en plus de l'authentification, ou service TM COMSEC
- L'un des critères majeurs est le niveau de Sécurité en regard des objectifs identifiés dans le document de référence de N. Bellare et N. Namprempprey
  - "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm" – 2007
  - **IND** : indistinguishability / **NM** : non-malleability
  - **CPA** : Chosen Plaintext Attack / **CCA** : Chosen Ciphertext Attack



Mode d'Opération de type AE (Authenticated Encryption)

- L'analyse de N. Bellare et N. Namprempprey montre qu'il est recommandé d'utiliser des modes d'opération AE de type "Encrypt Then MAC" => critère IND-CCA

Composition Method	Privacy			Integrity	
	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	insecure	secure	insecure
MAC-then-encrypt	secure	insecure	insecure	secure	insecure
Encrypt-then-MAC	secure	secure	secure	secure	secure

- Modes AE Candidats (Rapport ENISA)

Scheme	IND-CPA	IND-CVA	IND-CCA	Notes
Authenticated Encryption				
Encrypt-then-MAC	✓	✓	✓	Assuming secure Encrypt/MAC used
OCB	✓	✓	✓	
CCM	✓	✓	✓	
EAX	✓	✓	✓	An improved version of CCM
CWC	✓	✓	✓	
GCM	✓	✓	✓	
MAC-then-Encrypt	✓	✗	✗	See Encrypt-then-MAC text
Encrypt-and-MAC	✓	✗	✗	See Encrypt-then-MAC text

Mode d'Opération de type AE (Authenticated Encryption)

- Mode Encrypt-Then-Mac également requis par ANSSI
- Modes Encrypt-And-MAC / MAC-Then-Encrypt : utilisés initialement dans les premieres versions de SSL (Secure Socket Layer) ou SSH (Secure Shell)
- Modes d'Opération AE (Encrypt-Then-Mac) actuellement retenus pour les applications spatiales
  - GCM : Gallois Counter Mode - NIST SP800-38D
  - EAX : ISO/IEC 19772
  - EAX2
  - OCB : Offset CodeBlock

Mode d'Opération de type AE (Authenticated Encryption)

- Remarques sur les modes AE candidats
  - GCM
    - Très large déploiement et adoption (Réseaux, Internet, Informatique bancaire, ..)
    - Standard NIST, ISO, RFC, inclus dans la liste NSA Suite-B Cryptography
    - Faiblesse liée aux impacts d'une collision d'IV : risque de compromission de la clé GHASH et de ce fait , ouverture à des attaques de type bit-flipping sur le mode CTR
    - Impact opérationnel (Sol) important dans les systèmes spatiaux pour éviter la collision d'IV
      - L'IV Sol est contrôlé par l'Operateur SCC via l'IHM
      - Une erreur humaine / Opérateur (rejeu valeur IV antérieure) est toujours possible
    - Taille effective du MAC réduite à 96 bits dû à la découverte de clés GCM faibles
    - Performant , mais 75% du processing est dû à la fonction Authentification / GHASH
      - 25 % pour la fonction Chiffrement (CTR)

6 – Algorithmes cryptographiques et Modes d'Opération

- Remarques sur les modes AE candidats (suite)
  - EAX
    - Combinaison de 2 modes sûrs et performants : CTR et UMAC
    - Remplace avantageusement le mode CCM (standardisé par le NIST)
    - Mode non standardisé NIST
  - EAX2
    - Seul mode AE permettant l'utilisation de 2 clés distinctes : Authentification et Chiffrement
    - Séparation des clés (1 fonction = 1 clé) recommandé par l'ANSSI (RGS)
  - OCB
    - Mode très performant mais soumis à brevet ou sinon avec restrictions
      - Implémentation logicielle, utilisation non gouvernementale
- Compétition en cours **CAESAR** : émergence des modes AE futurs destinés à succéder avantageusement au mode GCM

Mode d'Opération de type EO (Encryption Only)

- Applicable pour la protection de flux Audio-Vidéo (liaisons de type AOS) où l'authentification n'est pas considérée / requise
- Modes AE candidats (NIST SP800-38A)
  - CTR : Counter Mode
  - CBC : Cipher Block Chaining Mode – en version sans padding
    - Note il existe des versions de CBC sans padding => CBC-CTS : ciphertext stealing
  - CFB: Cipher Feedback Mode
- Rapport ENISA sur les modes EO

Scheme	IND-CPA	IND-CVA	IND-CCA	Notes
Block Cipher Modes of Operation				
OFB	✓	(✓)	✗	No padding
CFB	✓	(✓)	✗	No padding
CTR	✓	(✓)	✗	No padding
CBC	✓	✗	✗	
ECB	✗	✗	✗	See text
XTS	-	-	✗	See text
EME	-	-	✗	See text

Sélection des primitives cryptographiques pour modes AO, AE, EO

- mode d'Opération HMAC : utilisation des primitives SHA-xxx
- Tous les autres modes d'opération sont basés sur une primitive Block Cipher
  - Aujourd'hui AES (NIST FIPS 197) est la primitive recommandée et utilisée
  - Autres primitives Block Cipher 128 : CAMELLIA ou SEED , alternatives envisageables
- Consultation d'avis issus d'organismes effectuant un survey / rapport annuels
  - ENISA, NIST, NSA, ANSSI , ECRYPT

Primitive	Classification	
	Legacy	Future
AES	✓	✓
Camellia	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
Blowfish$^{\geq 80}$-bit keys	✓	✗
DES	✗	✗

Table 3.2: Block Cipher Summary

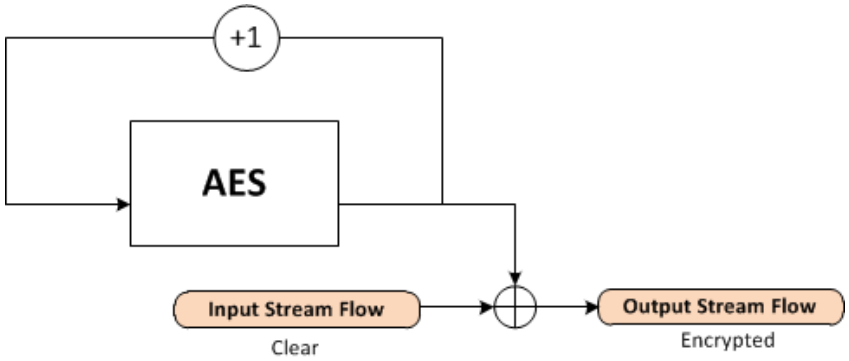
Primitive	Output Length	Classification	
		Legacy	Future
SHA-2	256, 384, 512	✓	✓
SHA3	256,384,512	✓	✓
Whirlpool	512	✓	✓
SHA3	224	✓	✗
SHA-2	224	✓	✗
RIPEMD-160	160	✓	✗
SHA-1	160	✓[1]	✗
MD-5	128	✗	✗
RIPEMD-128	128	✗	✗

Table 3.3: Hash Function Summary

Cas des Stream Cipher

- Pas de Stream Cipher recommandé par le CCSDS
- Echec des algorithmes Stream Cipher candidats lors de la consultation NESSIE
- Faille de l'algorithme RC4 utilisé initialement dans SSH
- On peut utiliser des Block Cipher pour faire du stream Cipher (ex: CTR, CFB)
  - COMSEC TM-HK ou COMSEC TM-PL
  - Voir exemple ci-joint
- Modes Candidats déjà analysés
  - HC-128
  - SALSA-20

Primitive	Classification	
	Legacy	Future
HC-128	✓	✓
Salsa20/20	✓	✓
ChaCha	✓	✓
SNOW 2.0	✓	✓
SNOW 3G	✓	✓
SOSEMANUK	✓	✓
Grain	✓	✗
Mickey 2.0	✓	✗
Trivium	✓	✗
Rabbit	✓	✗
A5/1	✗	✗
A5/2	✗	✗
E0	✗	✗
RC4	✗	✗



Taille Clés et MAC

Taille de clé de 128 bits convient en théorie à toutes les missions

- Mais pour les Clients exigeants (Opérateurs majeurs) ou Gouvernementaux, il n'y a pas vraiment de débat
  - La taille de clé de 256 bits est exigée de-facto
  - Indépendamment des analyses et démonstrations de robustesse de systèmes utilisant une clé de 128 bits
- À terme taille 256 bits pour l'AES imposée par la menace des ordinateurs quantiques

Taille de MAC : 128 bits acceptable – Evolution future à 256 bits

	Parameter	Legacy	Future System Use	
			Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size	m	80	128	256*
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(p^{k \cdot n}) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512

Taille de clés - autres sources

ANSSI : Recommandation 2014

Date	Symétrique	Factorisation Module	Logarithme discret Clef	Logarithme discret Groupe	Courbe elliptique GF(p)	Courbe elliptique GF(2^n)	Hash
2014 - 2020	100	2048	200	2048	200	200	200
2021 - 2030	128	2048	200	2048	256	256	256
> 2030	128	3072	200	3072	256	256	256

Les tailles de clef sont exprimées en bit. Ces résultats garantissent une sécurité minimale.
Cliquer sur une valeur pour la comparer avec les autres méthodes.

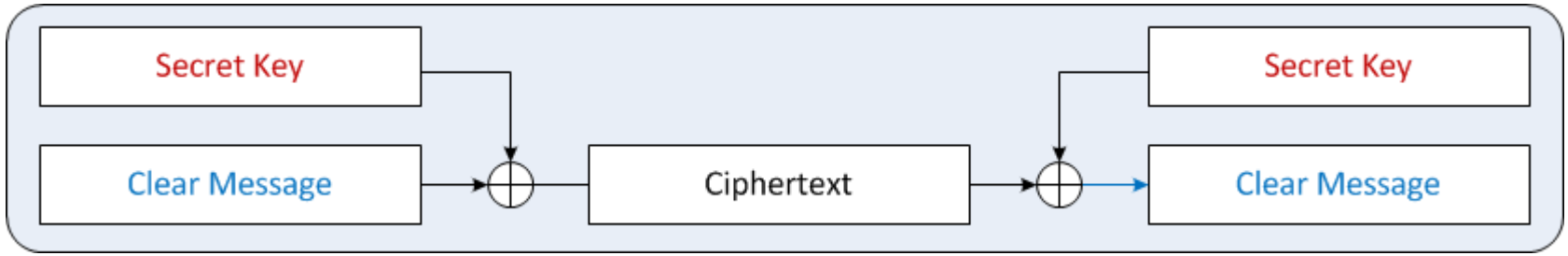
NSA : Suite B Cryptography

Type	Symétrique	Courbe elliptique	Hash
Secret	128	256	256
Top Secret	256	384	384

Les tailles de clef sont exprimées en bit. Ces résultats garantissent une sécurité minimale.
Cliquer sur une valeur pour la comparer avec les autres méthodes.

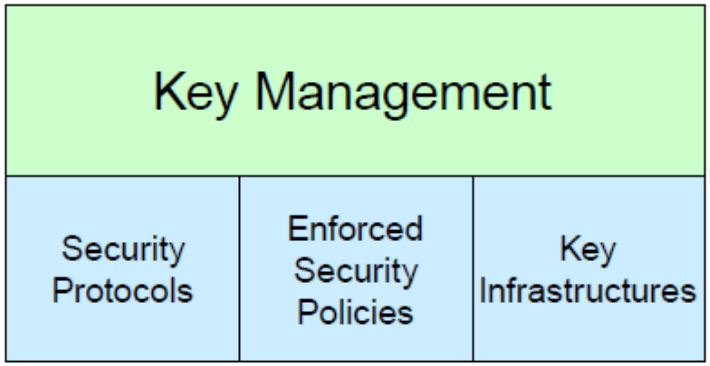
SKI : Chiffrement parfait : OTP (One Time Pad)

- Méthode de chiffrement inventée par Vernam (1917)
- 1 clé aléatoire, différente pour chaque message et de la taille du message à chiffrer
- Démonstration par Shannon en 1949 : Sécurité théorique absolue
  - Sécurité inconditionnelle
- Très rarement utilisé : complexité de la gestion associée des clés



7 – Gestion des Clés

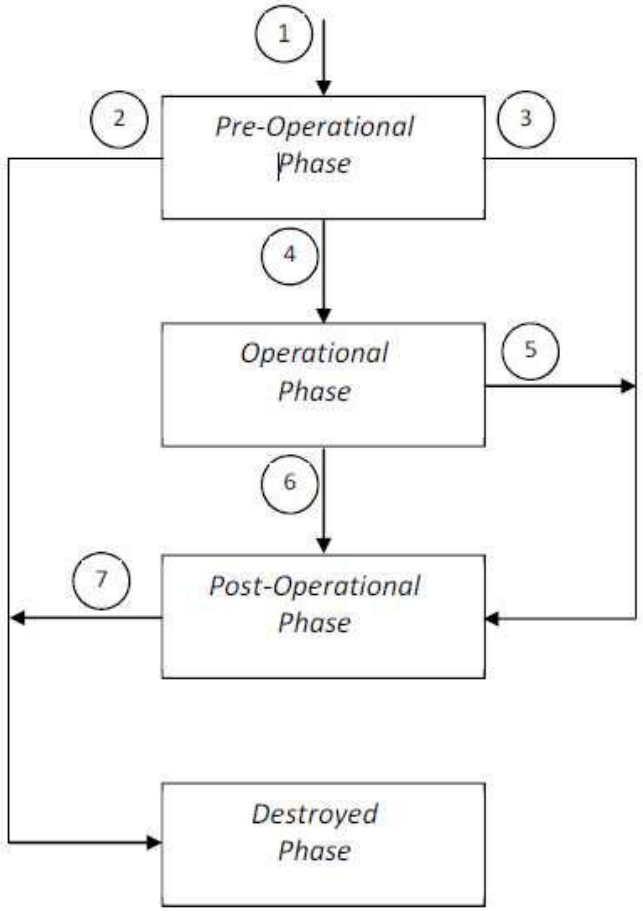
- Modèle de référence CCSDS pour la Gestion des Clés
  - Ref: CCSDS 350.6-G-1



- Trois blocs fonctionnels principaux
  - Security Protocols
    - Unilateral / mutual authentication
    - Key Establishment
    - Ex: IKE / IPSEC, SST-TLS, SSH, NIST KE schemes
  - Security Policies
    - operational procedures required for proper key management
    - Covers generation & distribution of cryptographic keys
  - Key Infrastructures
    1. Secret Key infrastructure (SKI)
    2. Public Key Infrastructure (PKI)

Cycle de Vie des Clés : Modèle de Référence NIST : SP800-57

- **Pre-Operational Phase**
  1. System and User Initialization;
  2. Entity Registration;
  3. Keying-Material Installation;
  4. Key Establishment;
  5. Key Registration.
- **Operational Phase**
  1. Normal Operational Storage Function;
  2. Continuity of Operations Function;
  3. Key Change Function;
  4. Key Derivation Function.
- **Post-Operational Phase**
  1. 1. Key Archive;
  2. 2. Key Recovery;
  3. 3. Entity De-registration Function;
  4. 4. Key De-registration Function;
  5. 5. Key Destruction Function;
  6. 6. Key Revocation Function.
- **Destroyed Phase**



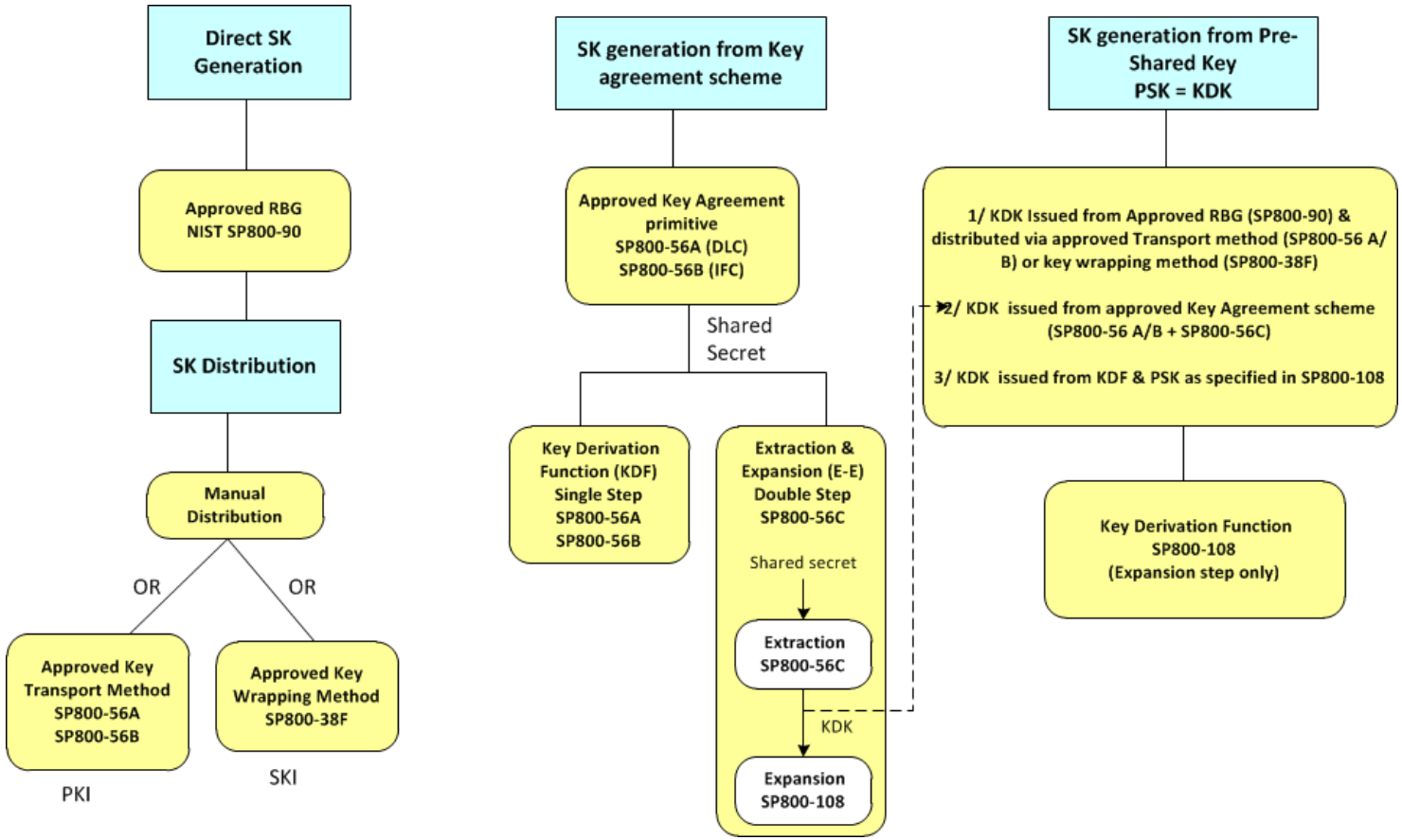
7 – Gestion des Clés

La Gestion des Clés relatives à la protection des liaisons spatiales et basées sur la cryptographie SKI inclut les phases suivantes

- Génération des clés COMSEC ou TRANSEC
  - Clés de Trafic, Clés de wrapping (KEK : Key Encryption Key) pour le renouvellement en Vol (OTAR)
  - OTAR : Over The Air Rekeying
- Distribution sécurisée des Clés au Sol
  - Protection par une clé de wrapping Sol (GPK : Ground Protection Key)
- Chargement des Clés dans le satellite avant le Tir (Injection des clés)
- Gestion des clés durant la mission / exploitation du satellite
  - Changement régulier de clé : suivant la crypto-période choisie
  - Renouvellement en vol (OTAR)
  - Invalidation / effacement de Clé
    - clé obsolète – crypto période expirée ou clé compromise

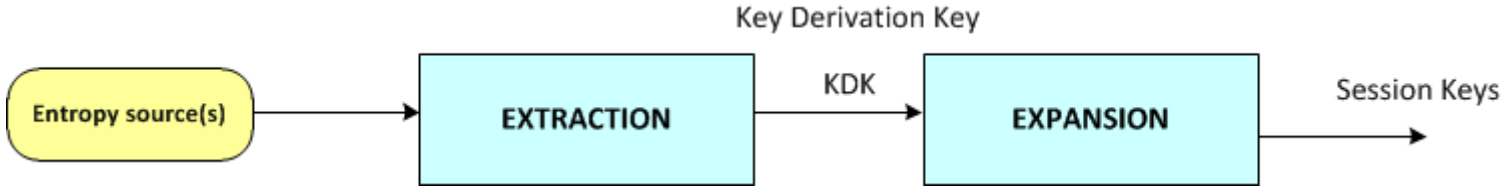
❑ Génération des clés Symétriques COMSEC ou TRANSEC

- Reference NIST : SP800-133 : Key Generation



❑ Dans les solution actuelles basées sur la technologie Full SKI

- ➢ Les clés de trafic sont générées par un PRNG
  - Pseudo-Random Number Generator
  - Modèle E-E
    - **E**xtraction de l'Entropie
    - **E**xpansion / dérivation des clés

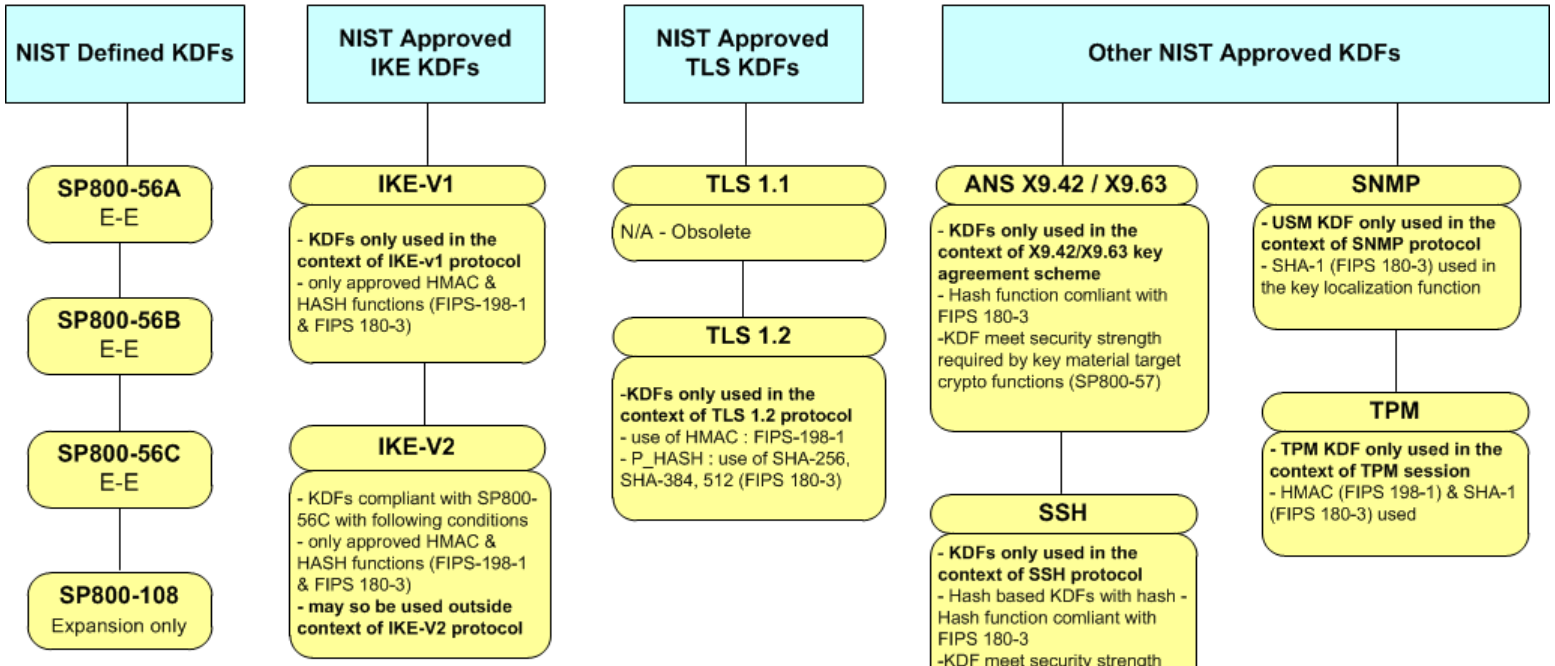


- ➢ Les clés sont protégées par une clé de wrapping
  - Ex standard NIST SP800-38F pour algorithme Key Wrapping
  - Pas de distribution de clés rouges (claires) au sol

❑ Génération des clés symétriques COMSEC ou TRANSEC

➢ Référence NIST : SP800-135 : Key Derivation Functions

NIST SP800-135 Recommended KDFs



E-E : Extraction & Expansion

❑ Gestion des Clés de Trafic (SKI) en Vol

- ➢ Changement régulier de clé : selon une crypto-période à définir (ex: 1 mois)
  - la crypto-période est davantage liée aux risques d'exposition et de compromission de clés au Sol que liée aux exigences cryptographiques
  - avec un mode AO ou AE utilisant l'AES, la limite théorique est définie par le nombre d'appels AES qui pour une clé donnée ne doit pas dépasser 2^64
    - Recommandation ANSSI : nombre d'appels < 2^48
  - Autres contraintes cryptographiques
    - crypto période < période du compteur anti-rejeu
    - crypto période < période de l'IV
- ➢ Renouvellement des Clés en Vol : service OTAR
  - Upload d'un jeu de clés protégées par une Clé de wrapping / KEK
  - Intérêt : génération et upload de clés fraiches le plus tard possible durant la mission – limitation de la compromission
  - Remplacement de clés bord corrompues (ex: SEU)

❑ Limites de la technologie SKI pour la Gestion des Clés

➢ Impacts de la compromission des clés su Sol

- Pas de recouvrement possible des clés satellite si compromission des clés au Sol
- Pas de PFS (Perfect Forward Secrecy) si le jeu de KEK à bord est compromis
  - PFS : confidentialité des échanges anterieurs restent garantis si une clé courante est compromise
  - PFS non compatible de clés long terme (KEK) utilisées pour la confidentialité

➢ Limites de l'Injection des clés dans le satellite

- Chargement des clés en clair si état initial = pas de clé secrète / partagée à bord
- Canal d'injection non protégé => Protection par des mesures radio-fréquence (protection TEMPEST)
- Pas d'authentification possible de l'équipement d'injection des clés par le satellite
  - On ne peut par design, garantir à un Client qu'il est le seul capable de charger des clés dans le satellite
- Protection par des mesures classiques (ex: scellé, vidéo) et organisationnelles

❑ Limites de la technologie SKI pour la Gestion des Clés

➢ Complexité de la Gestion des Clés Multi-Utilisateurs

- Mission Observation : jusqu'à 1000 utilisateurs Sol
- La gestion des clés TM-PL COMSEC obéit à des contraintes de nature dynamique (enregistrement, début / Fin du service, révocation)
- Avec les solutions SKI, l'utilisation de clés partagées ne permet pas de lien formel possible entre l'Identité d'un Utilisateur et une Clé donnée
- Faible flexibilité

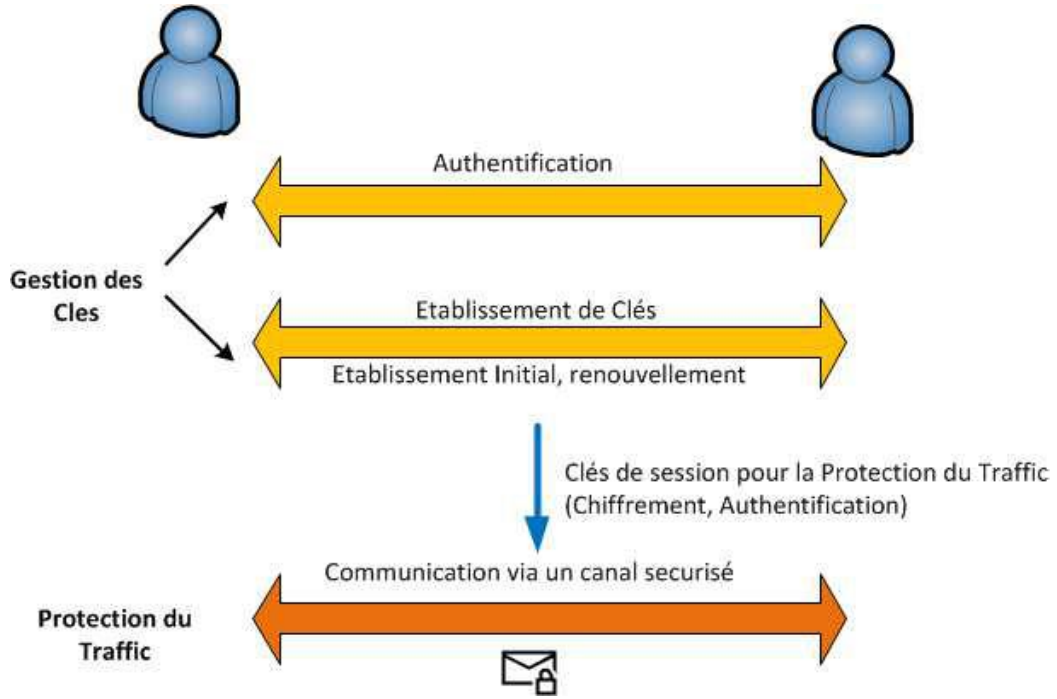
- Implémentation de la technologie PKI pour la Gestion des clés
  - Permet de solutionner les défauts / limitations de la technologie SKI
  - Existence de Nombre de protocoles dits d'Etablissement de Clés (KE : Key Establishment) standards sans aucune clé secrète partagée au préalable
    - KE couvre 2 types de protocoles: Key Agreement (KA) et Key Transport (KT)
      - KA : Key Agreement ; établissement sécurisé de clés secrètes SKI durant la session
      - KT : Key Transport :, établissement durant la session, d'un canal sécurisé puis transport à travers ce canal, de clés secrètes SKI préalablement générées
    - Standards KE du NIST
      - SP800-56 A (DLC) : Discrete Logarithm Cryptography
      - SP800-56B (IFC) : Integer Factorization Cryptography
    - Protocole d'établissement de clés (KE) spécifiques
      - SSL/TLS (TLS 1.2)
      - IPSEC (IKE) : Internet Key Exchange
      - Protocoles KE : RSA, DSA, DHE-RSA, DSS-RSA, ECDHE-RSA
      - Seuls les protocoles KE utilisant des clés éphémeres garantissent la PFS

- Implémentation de la technologie PKI pour la Gestion des clés
  - Fonctions cryptographiques utilisées par les protocoles KE
    - Chiffrement: RSA-OAEP
      - Taille de clé (modulus N) : ≥ 3072 bits
      - Taille du plaintext < taille du modulus N
      - Taille du ciphertext : taille du modulus
    - Signature digitale (permettant la non répudiation): DSS, RSASSA
      - Non répudiation: l'auteur d'un message signé ne peut le renier car lui seul est capable d'avoir généré la signature accolée au message avec sa clé privée (PRK) et ceci peut-être démontré (y compris devant un tribunal)
  - Primitives cryptographiques utilisées par les fonctions cryptographiques
    - RSA, DSA, ECDSA, Diffie Hellman, MQV, IBE, RSA-KEM…
    - RSA-KEM : intérêt pour la distribution des clés TMI

7 – Gestion des Clés

- Le standard DSS (FIPS 186-4) specifie 3 algorithmes
  - DSA
  - RSA
  - ECDSA
- DSA
  - Taille max de clé : 3072 bits (L = length of prime modulus)
  - Taille max de signature : 256 bits (N = length of q prime divisor of p)
- RSA
  - Taille max de clé : 3072 bits (L = length of prime modulus)
  - Taille max de signature : 3072 bits (L = length of prime modulus)
- ECDSA
  - Taille max de clé : 512 bits (n = order of G point)
  - Taille max de signature (r, s) => 2 x 512 bits

- Implémentation de la technologie PKI pour la Gestion des clés
  - Une session KE inclut 2 étapes principales
    - Etape 1 – Authentification (mutuelle ou unilatérale)
    - Etape 2 – génération des clés de session pour la protection du Trafic



7 – Gestion des Clés

Session KE : Etape 1 – Authentification (mutuelle ou unilatérale)

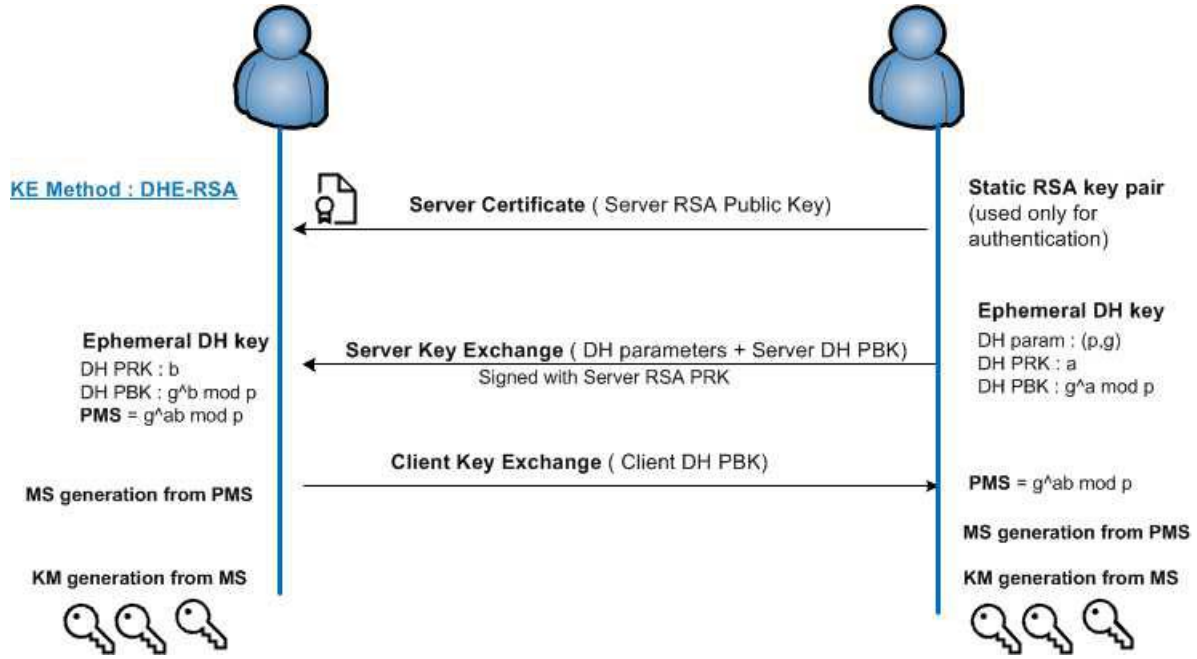
- Echange de certificats PBK (Public Key) et permettant d'authentifier tous les échanges en Etape 2 via la vérification de la signature digitale
  - Ex: algorithme RSA, DSA ou ECDSA

Session KE : Etape 2 – génération des clés de session (protection du Trafic)

- Etablissement d'un secret commun , puis dérivation des cles de session à partir du secret commun via une fonction de dérivation KDF
- Une cryptographie forte requiert des protocoles et algorithmes garantissant la PFS (Perfect Forward Secrecy) : confidentialité des communications passées (session KE antérieures) garanties en cas de compromission d'un secret lie à une session KE actuelle
- De ce fait l'établissement du secret commun ne peut en aucun cas se baser sur des clés longue durée et archivées mais uniquement sur des clés ephémères
- Cas du standard SSL-TLS
  - Protocole KE RSA : ne garantit pas la PFS
  - Protocoles DHE-RSA, ECDHE-RSA, DHE-DSS : garantissent la PFS

Exemple de Session KE avec PFS : SST-TLS avec protocole KE DHE-RSA

- Authentification via RSA et clé longue durée (compatible PFS)
- Secret commun (PMS : pre-master secret) via algorithme DHE : Ephemeral Diffie Hellman => PFS
- MS (Master Secret) et Key material (Cles de Session) générées à partir de PMS via la cryptographie symétrique)



7 – Gestion des Clés

NIST SP800-56A => Key Agreement Protocols		
	KA Protocols	**Primitives**
C(2e, 2s)	dhHybrid1	FFC-DH
	Full Unified Model	ECC-CDH
	MQV2	FCC-MQV
	Full MQV	ECC-MQV
C(2e, 0s)	dhEphem	FFC-DH
	Ephemeral Unified Model	ECC-CDH
C(1e, 2s)	dhHybridOneFlow	FFC-DH
	One-Pass Unified Model	ECC-CDH
	MQV1	FFC-MQV
	One-Pass MQV	ECC-MQV
C(1e, 1s)	dhOneFlow	FFC-DH
	One-Pass Diffie-Helmann	ECC-CDH
C(0e, 2s)	dhStatic	FFC-DH
	Static Unified Model	ECC-CDH
NIST SP800-56A => Key Transport Protocols		
	Protocol	**Primitives**
One KT defined	KA scheme : subset of C(2e, 2s), C(1e, 2s), C(1e, 1s), C(0e, 2s)	Subset of primitives listed above

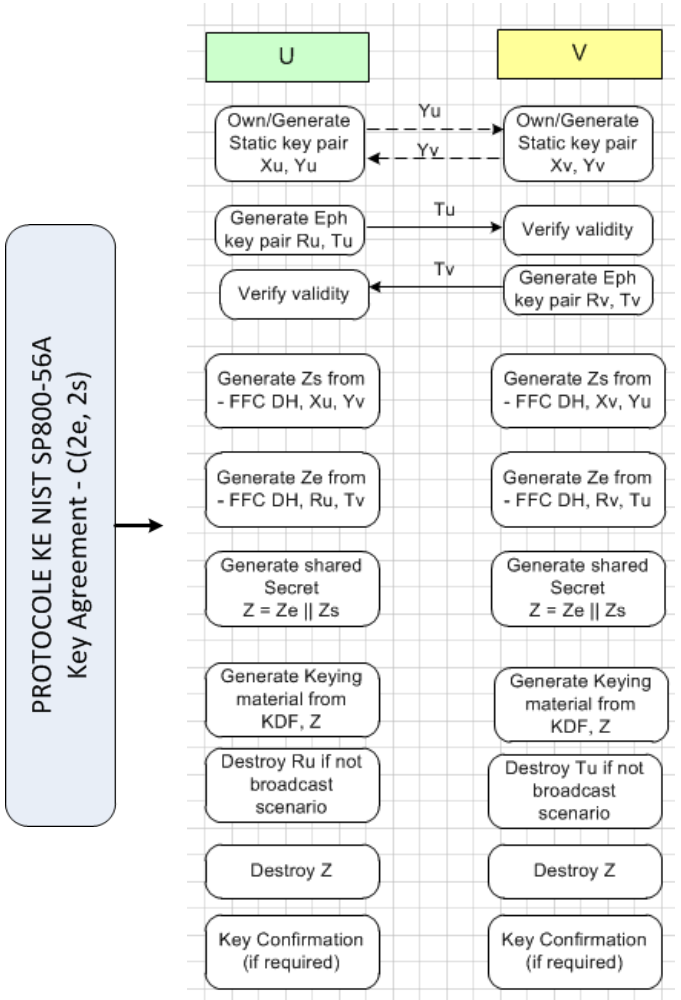
Protocoles et Primitives KE du NIST

- C(ne, ps) : nombre de pair de clés PBK / PRK statiques / ephemères

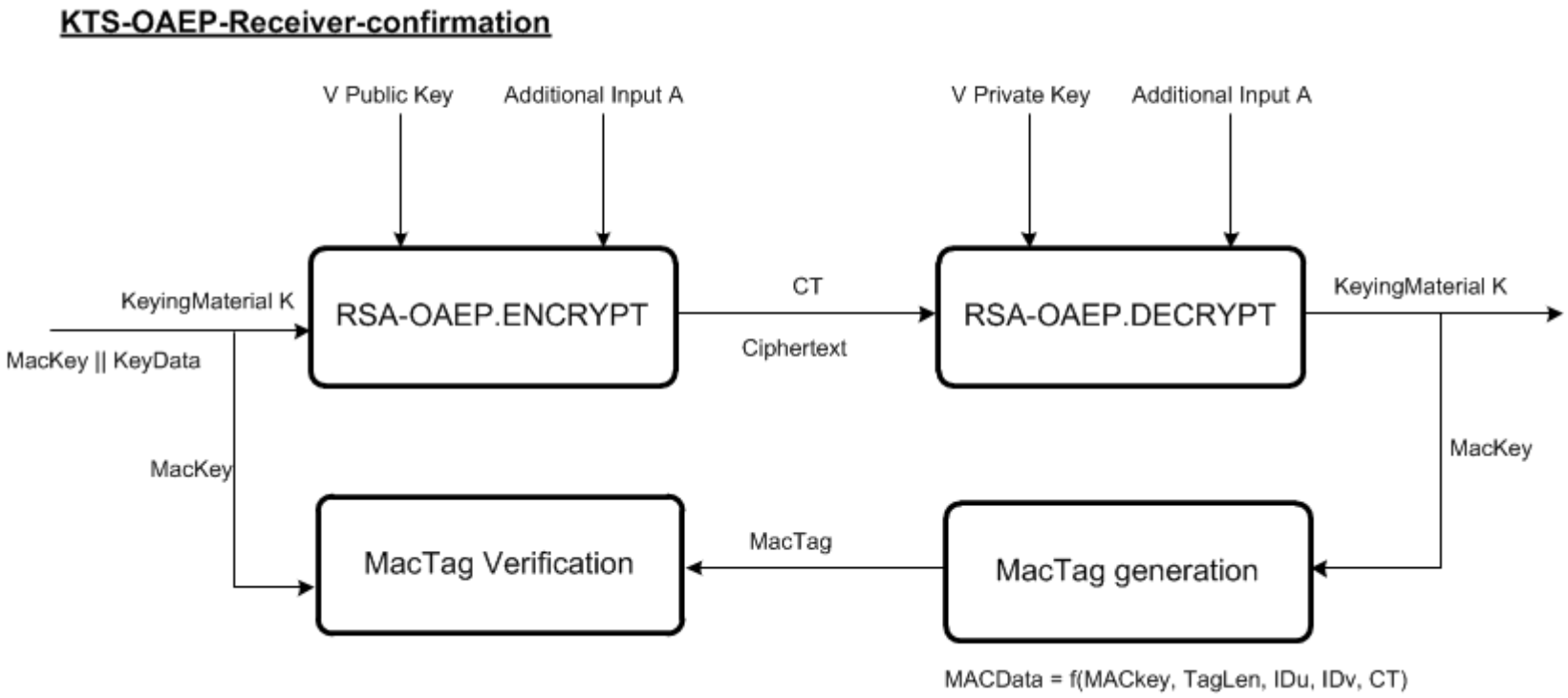
NIST SP800-56B => Key Agreement Protocols	
KA Protocols	**Primitives**
KAS1-basic	RSASVE (RSA EP/DP)
KAS1-responder–confirmation	RSASVE
KAS2-basic	RSASVE (RSA EP/DP)
KAS1-responder–confirmation	RSASVE
KAS1-initiator–confirmation	RSASVE
KAS2-bilateral–confirmation	RSASVE
NIST SP800-56B => Key Transport Protocols	
KT Protocols	**Primitives**
KTS-OAEP-basic	RSA-OAEP
KTS-OAEP-receiver-confirmation	RSA-OAEP
KTS-KEM-KWS-basic	RSA-KEM-KWS
KTS-KEM-KWS-receiver-confirmation	RSA-KEM-KWS

Exemple de Session KE basée sur un protocole KE du NIST

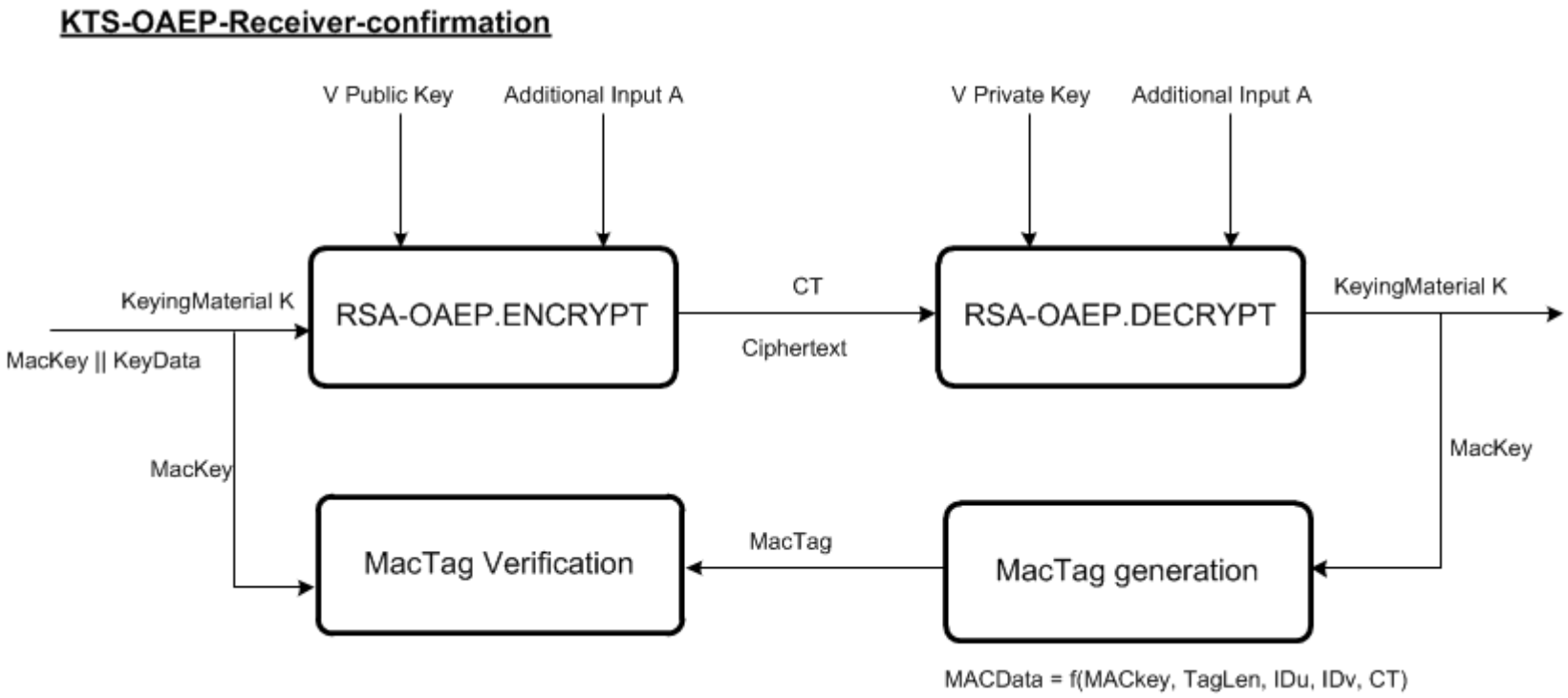
- *Standard SP800-56A (DLC)*
- *Protocole KA (Key Agreement)*
- *Protocole C(2e, 2s) avec authentification mutuelle et confirmation de clé*



- NIST SP800-56B (IFC):
  - Protocole Key Transport – KTS-OAEP avec Key Confirmation



- NIST SP800-56B (IFC):
  - Protocole Key Transport – KTS-OAEP avec Key Confirmation



❑ Cryptographie: Menaces liées à l'avènement des ordinateurs quantiques

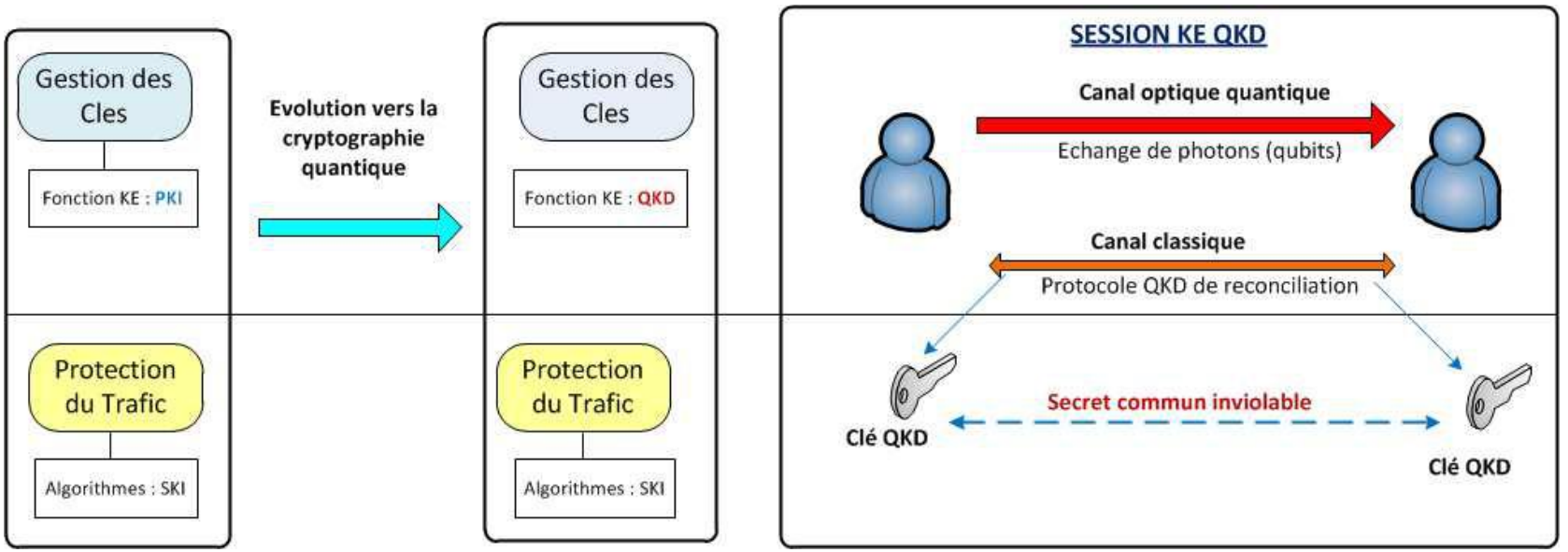
- ➢ La cryptographie asymétrique **(PKI)** est basée sur une sécurité **conditionnelle**
  - Les algorithmes PKI reposent sur 2 problèmes mathématiques réputés « difficiles »
    - DLC : Logarithme discret (Diffie Hellman, Courbes elliptiques)
    - IFC : Factorisation des grands nombres (RSA)
  - La sécurité de la cryptographie asymétrique (PKI) se base sur l'hypothèse (difficulté calculatoire) que ces deux problèmes ne peuvent être résolus avec les moyens actuels et dans des délais suffisamment courts pour menacer la mission concernée
  - Cette hypothèse va progressivement être battue en brèche avec l'avènement des ordinateurs quantiques utilisant l'algorithme de Shor
- ➢ La cryptographie symétrique (SKI) est également basée sur une sécurité **conditionnelle**
  - Cependant de par le design des algorithmes cryptographiques SKI, elle n'est pas considérée comme menacée par l'avènement des ordinateurs quantiques
  - Sous réserve d'utiliser des clés de 256 bits au minimum (ex avec AES)
- ➢ 2 solutions pour contrer la menace sur la PKI et la gestion des clés
  - Cryptographie quantique
  - Cryptographie post-quantique

❑ Cryptographie Quantique / QKD (Quantum Key Distribution)

- ➢ La cryptographie quantique est une alternative en plein développement, pour laquelle la sécurité repose sur des postulats physiques (physique quantique), par principe inviolables .
  - Elle permet au niveau de la génération et distribution des clés d'offrir une sécurité inconditionnelle se basant sur des impossibilités imposées par les lois de la physique quantique , et non plus sur la puissance supposée des moyens de calcul d'un tiers mal intentionné
  - garantie absolue de la confidentialité et de l'intégrité des clés échangées sur un canal optique non protégé, avec détection systématique de toute intrusion sur ce canal optique
- ➢ La cryptographie quantique définit une nouvelle fonction d'établissement des clés dite QKD (Quantum Key Distribution) garantissant une sécurité inconditionnelle des clés générées
- ➢ Elle se traduit au niveau des architectures de sécurité, par l'introduction d'une nouvelle primitive KE (QKD) au sein de la fonction de Gestion des Clés

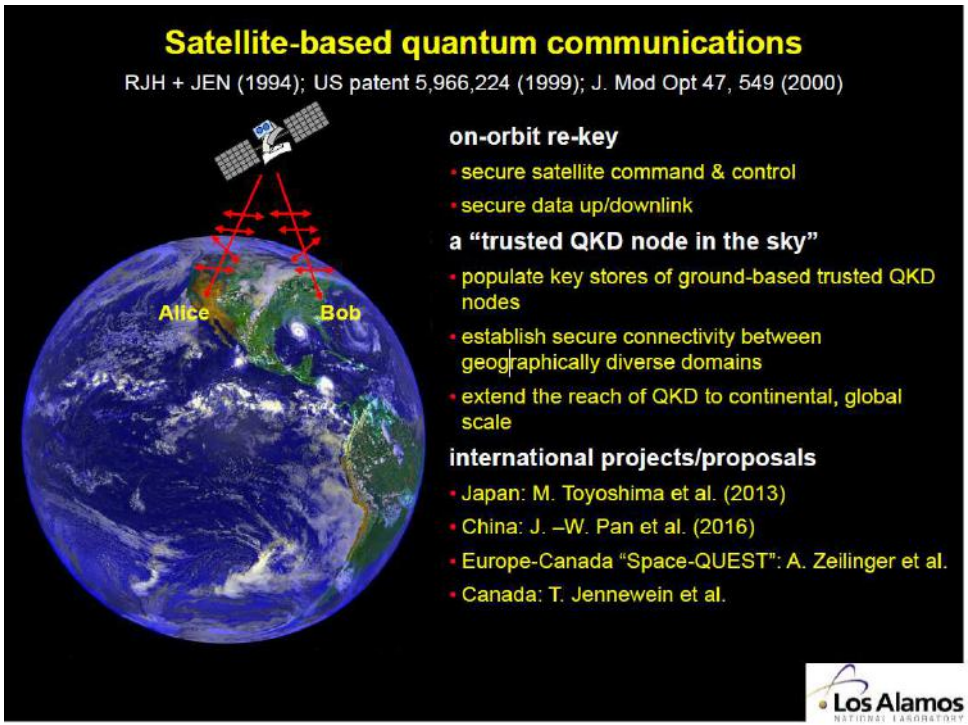
Introduction de la Cryptographie Quantique

Etablissement des Clés (Fonction KE) : Evolution PKI vers KQD



- Introduction de la Cryptographie Quantique
  - Application à l'établissement de clés en temps réel par liaison optique entre un satellite des stations Sol
  - De nombreux projets / démonstrateurs en cours – Buzz suite au lancement du premier satellite quantique par la Chine en juillet 2016

- Exemple d'application
  - Le satellite passe au-dessus de la station A et établit une clé KA via la QKD
  - Le satellite passe au-dessus de la station B et établit une clé KB via la QKD
  - Le satellite repasse au-dessus de la station A et transmet KA XOR KB
  - Les Sites A et B peuvent alors établir une communication sol sécurisée par la clé commune KB et considérée comme inviolable par la QKD



Cryptographie Post-quantique

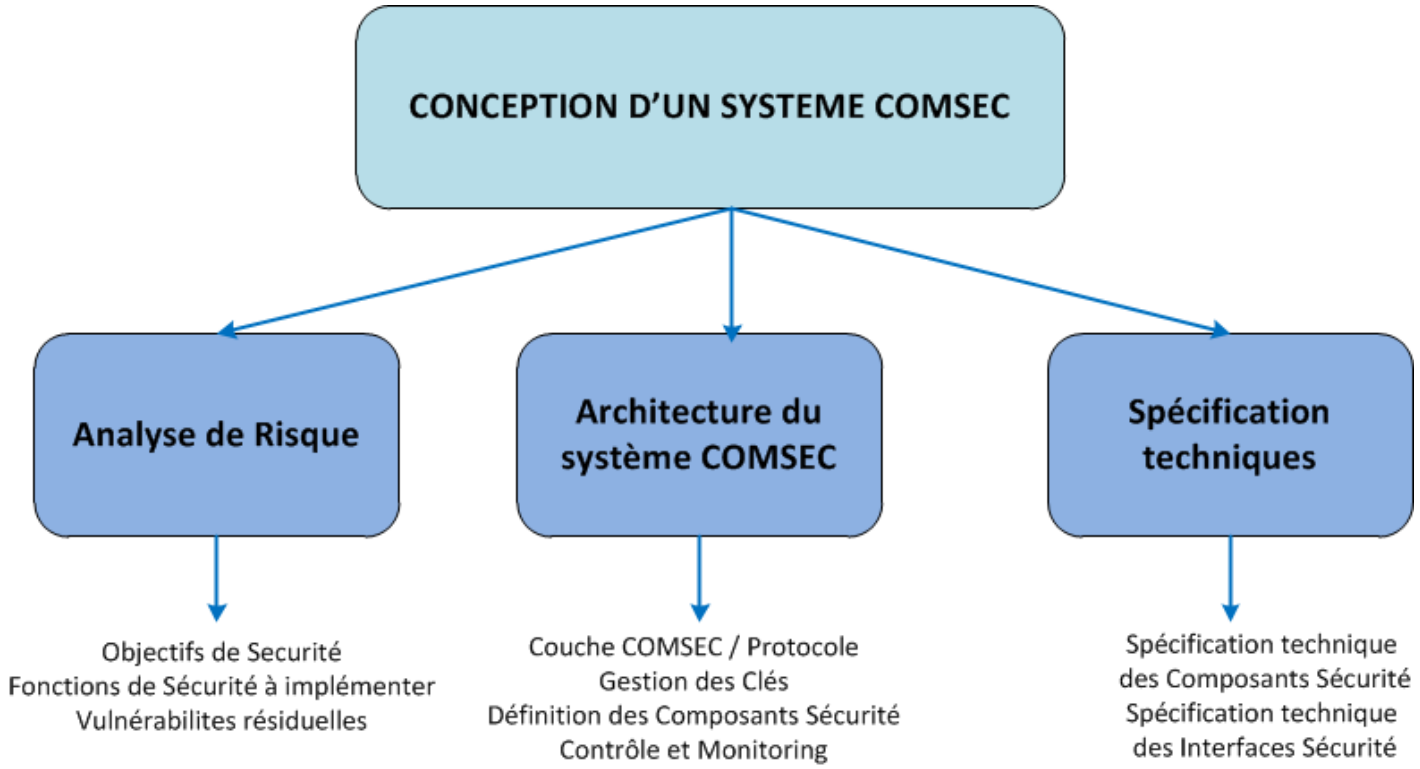
- Definition : la cryptographie post-quantique adresse les algorithmes cryptographiques capables de résister aux ordinateurs quantiques
- La cryptographie symétrique (SKI) n'est pas considérée comme menacée par les ordinateurs quantiques (utilisant l'algorithme Grover) si l'on utilise des cles de taille importante (ex: cles AES de 256 bits)
- Ca n'est pas du tout le cas de la cryptographie asymétrique (PKI) dont la sécurite repose sur l'hypothèse de complexite computationnelle et plus precisément sur 2 problèmes mathématiques reputés "durs"
  - Factorisation des grands nombres (> 2000 bits) => RSA
  - Logarithm Discret => Diffie Hellman, Elliptic curves
- Attaques possibles avec ordinateurs quantiques et utilisation de l'algorithme de SCHOR
  - La menace est actuellement contrée via l'accroissement des tailles de clé
  - Ex pour RSA : taille de clé (modulus) allant de 3072 bits au minimum et jusqu'à 15000 bits (recommandations ISO, IETF, NSA, BSI, ANSSI, ENISA, ECRYPT)

7 – Gestion des Clés

- Forte activité de recherche sur les ordinateurs quantiques
  - Existence des premiers ordinateurs quantiques (ex: D-WAVE) mais avec de fortes limitations
  - L'avènement des ordinateurs quantiques réèllement puissants et menacants est estimée à 20 ans
- Le développement des ordinateurs quantiques constitue une menace sérieuse pour la cryptographie asymétrique impliquant de considerer de futurs algorithmes PKI capables de resister à ces derniers
  - 2015 : Alerte de la NSA en direction de l'Administration US
  - 2016 : Initiative du NIST : competition pour le développement d'algorithmes PKI post-quantiques
  - Europe : activite de recherche (ETSI) sur les d'algorithmes PKI post-quantiques
- Implication progressive des Agences spatiales et Opérateurs satellites
  - pour assurer la sécurite sur le long terme des systemes spatiaux et preparer la migration des algorithmes PKI utilisés vers le post-quantique
- Principales activites de recherche sur la cryptographie post-quantique
  - Multivariate cryptography
  - Code-based cryptography
  - Euclidian Network / Code based Lattice cryptography
  - Hash-based cryptography

8 – Cas de Systèmes COMSEC pour la protection des liaison spatiales

❑ Activités de Conception d'un Système COMSEC



❑ Conception d'un Système COMSEC TM/TC

➢ Analyse de Risque - les sorties principales sont:

- Les fonctions / mesures de sécurité à implémenter sur la liaison spatiale (Authentification et/ou Chiffrement)
- Les vulnérabilités résiduelles : vulnérabilités non couvertes par les fonctions de sécurité identifiées, mais acceptables

➢ Architecture du Système COMSEC (1/2)

- Le protocole de la couche définit les interactions / échanges (handshake), et le format détaillé des messages échangés
  - Ex: le standard CCSDS Space Data Link Protocol, définit le format des champs Sécurité à appliquer aux messages TC ou TM à protéger
- Composants : équipement ou Fonction logiciel Bord & Sol
  - Chiffreur / Dechiffreur materiel bord ou Sol
  - Couche Logicielle bord ou Sol

Protocole : Couche TC / TM COMSEC

Avant 2015:

- Seul standard existant : TC Authentification ESA (ESA PSS-05-151)
- Toutes les solutions TC/TM Encryption sont forcément propriétaires

Depuis Sept 2015

- Le standard CCSCS CSDS est sorti officiellement en Issue 1
- Les principaux Clients / Opérateurs sont fortement intéressés à s'appuyer sur un standard garantissant l'interopérabilite entre satellites et segments sol issus de fournisseurs différents
- Le protocole de la couche définit les interactions / échanges (handshake), et le format détaillé des messages échangés
- Implémentation par TAS : solutions TC Encryption & TM Encryption

Secured Message Format with CCSDS SDLS Protocol Standard

Message Authentication Code (MAC)

- Standard CCSDS SDLS Fonction de Sécurité vs Paramètres Sécurité
  - Authenticité : MAC
  - Intégrité : MAC
  - Anti-rejeu : Compteur ARSN
    associé à une fenêtre anti-rejeu incluse dans le calcul du MAC
  - Confidentialité : Chiffrement
- Role des Paramètres / champs Sécurité
  - SPI : Security Parameter Index - Identifie une Security Association (SA)
  - IV : Initialization Vector utilisé par l'algorithme (ex: GCM, CBC, CTR)
  - ARSN : Anti Replay Sequence Number - compteur anti-rejeu
  - Pad length : taille des octets de bourrage si padding requis par l'algorithme
    - Ex: algorithme CBC-AES requiert du padding car il ne travaille que sur des blocs de données de 16 octets

❑ Activités de Conception d'un Système COMSEC

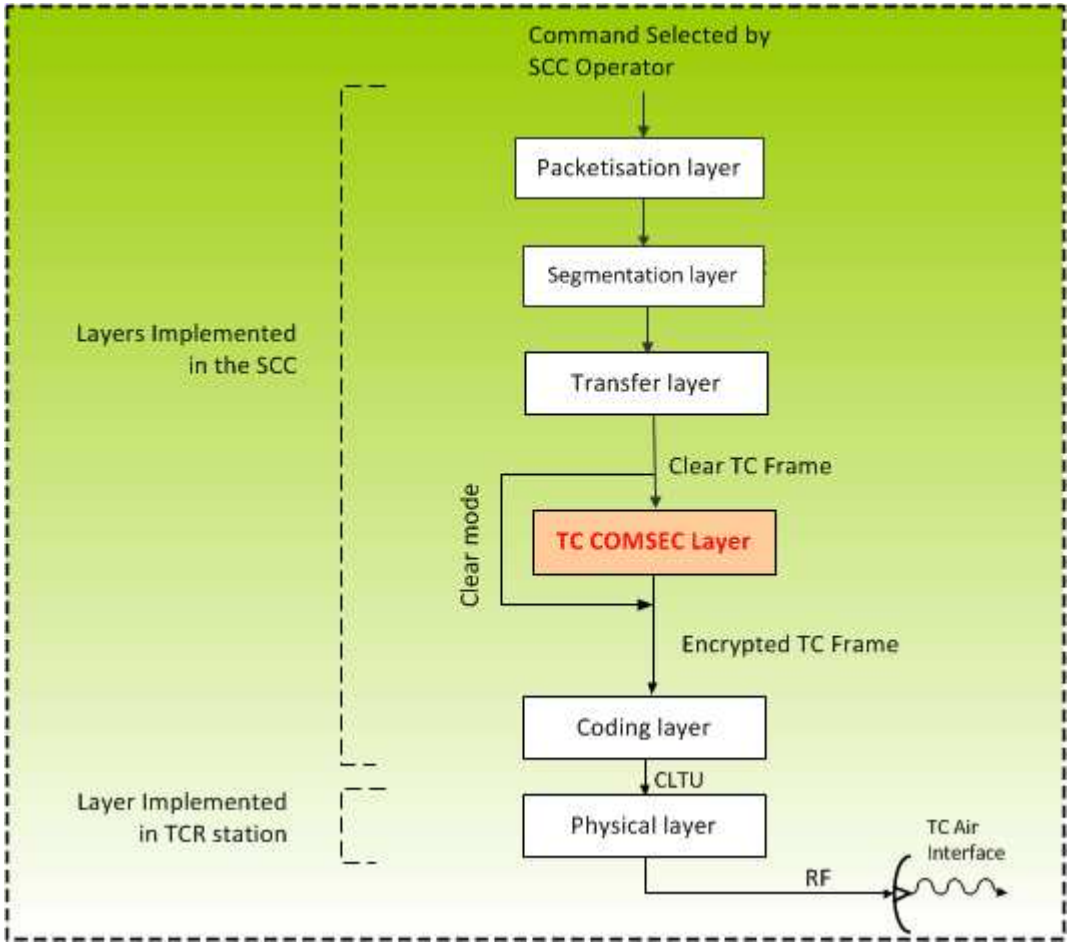
➢ Architecture du Système COMSEC

- La Gestion des Clés traite l'ensemble des fonctions à implémenter pour couvrir le cycle de vie des clés : génération, distribution, changement, renouvellement en vol, invalidation, stockage, protection, ..
- Les composants sont les constituants physiques (Sol et Bord) résultant de l'allocation des fonctions de sécurité
- Le contrôle et monitoring définit
  - Les commandes de contrôle et configuration de la fonction Securite bord
    - Activation de la sécurite (Secure mode), désactivation (Clear mode)
    - Changement de la cle courante
    - Modification du compteur anti-rejeu
    - Telechargement d'une clé en vol (OTAR : over the air rekeying)
  - Les informations de configuration / status / alarmes redesendues vers le sol et permettant une observabilité de la fonction Securite bord

• Specification Techniques

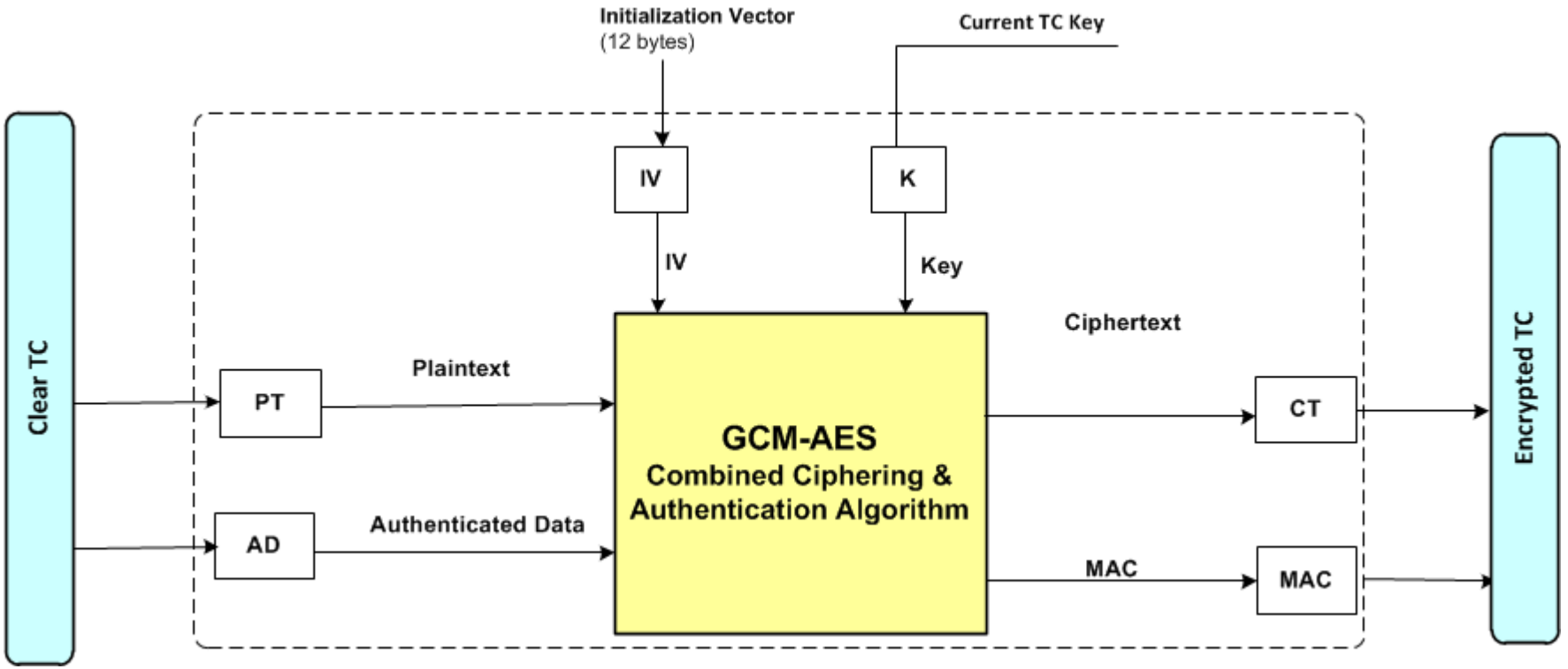
- Elaboration des exigences techniques des différents composants Sécurité ainsi que des interfaces associées, afin de permettre leur développement

- Exemple 1 : Système COMSEC TC
  - Positionnement de la Couche TC COMSEC
  - Exemple : Opération sur des Trames de Transfert

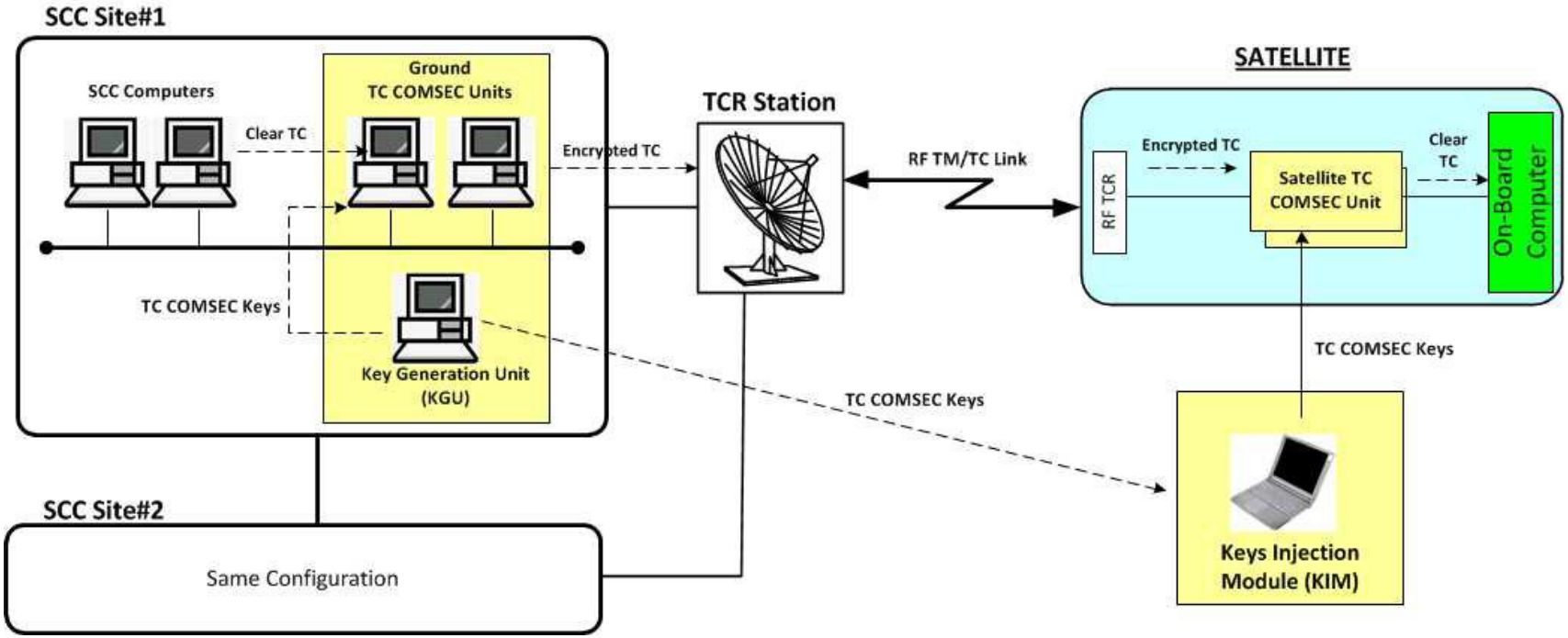


Exemple 1 : Système COMSEC TC

Définition de la fonction Encryption d'un message TC – Ex avec GCM-AES



❑ Exemple 1 : Système COMSEC TC – Configuration Système



- Exemple 1 : Système COMSEC TC
  - Composants Sol
    - Key Generation Unit : génération des clés (Clés de Traffic, KEK)
    - Ground TC COMSEC Unit : Chiffrement et authentification des TC
    - Key Injection Module : chargement des clés dans le satellite
  - Composants Bord / Satellite
    - Satellite TC COMSEC Unit : déchiffrement et authentification des TC
  - La conception des composants varie très fortement suivant le niveau de Sécurité applicable et la certification ou non des équipements concernés
    - Equipement Sécurité en coupure des flux à protéger
    - Séparation physique des ports E / S pour les données claires /chiffrées
    - Cloisonnement interne en zones rouges (manipulation des données claires) / noire (rouges (manipulation des données chiffrées)
    - Detection anti-intrusion
    - Gestion des Clés
    - Implementation des fonctions cryptographiques

Exemple 1 : Système COMSEC TC

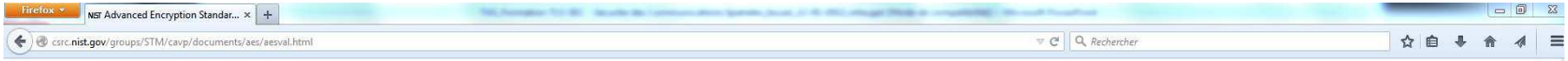
Certification Sécurité

- Certification Critères Commun (CC)
  - 7 niveaux d'Assurance Sécurité : EAL (Assurance Evaluation Level)
  - Evaluation par un organisme agréé dit CESTI (en France agréé par ANSSI)
  - Pour chaque équipement, l'evaluation se fait sur la base d'un document Cible de Sécurité (TOE : Target of Evaluation) incluant l'ensemble des exigences de sécurité à verifier
  - Inclut des tests de vulnérabilité poussés suivant le niveau EAL
- Certification NIST
  - Basé sur les exigences définies dans le document NIST FIPS 140-3
  - 4 niveaux d'assurance sécurité
  - Evaluation par un organisme / laboratoire agrée par NIST

Validation de l'implémentation de l'algorithme cryptographique

- Process courant NIST avec l'algorithme AES
- Validation réalisée par un Labo agréé NIST
- Verification du Code, Execution de Test patterns complets
- À la fin : inscription dans l'AES Validation List officielle du NIST

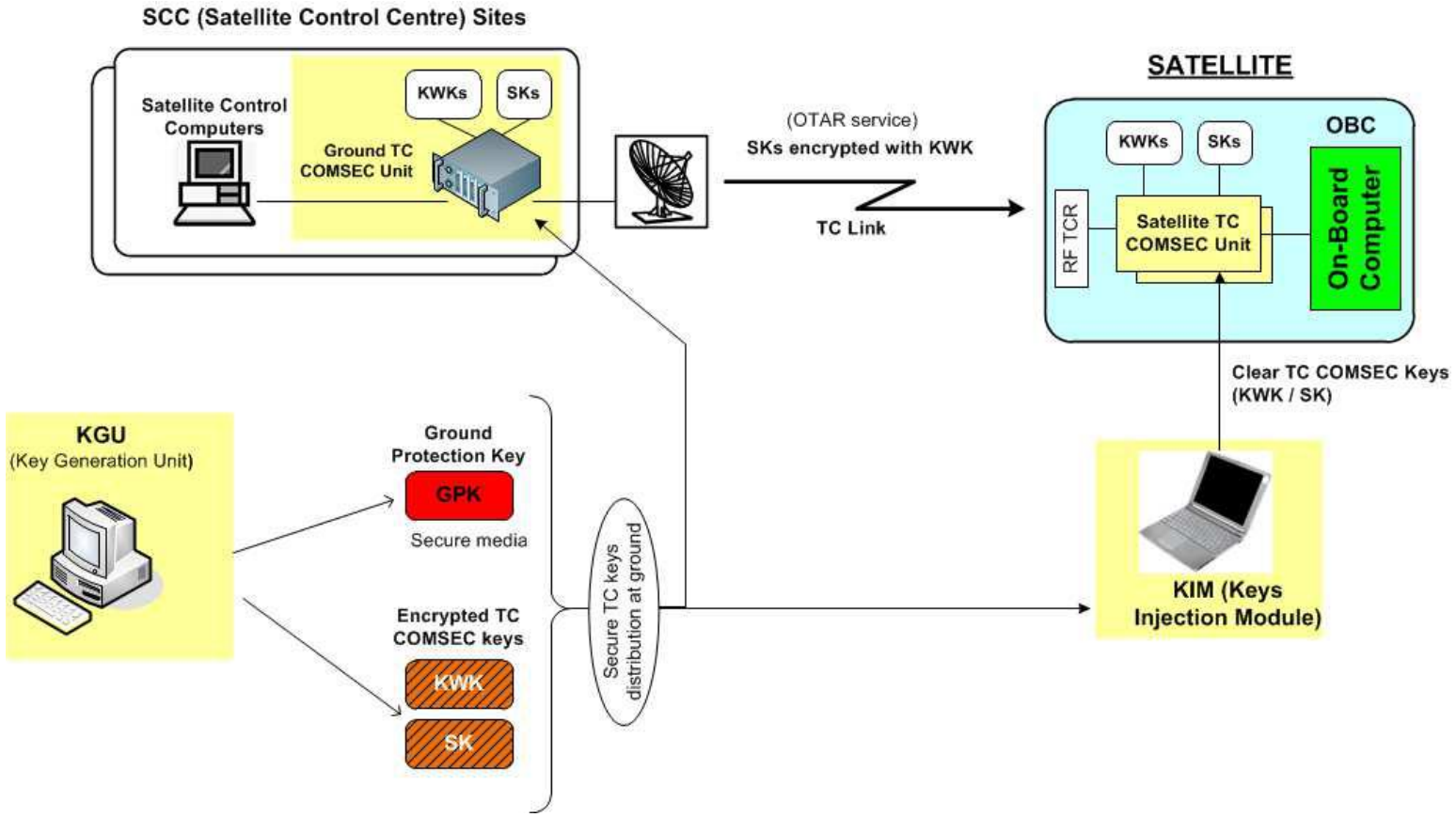
❑ NIST : AES Validation List



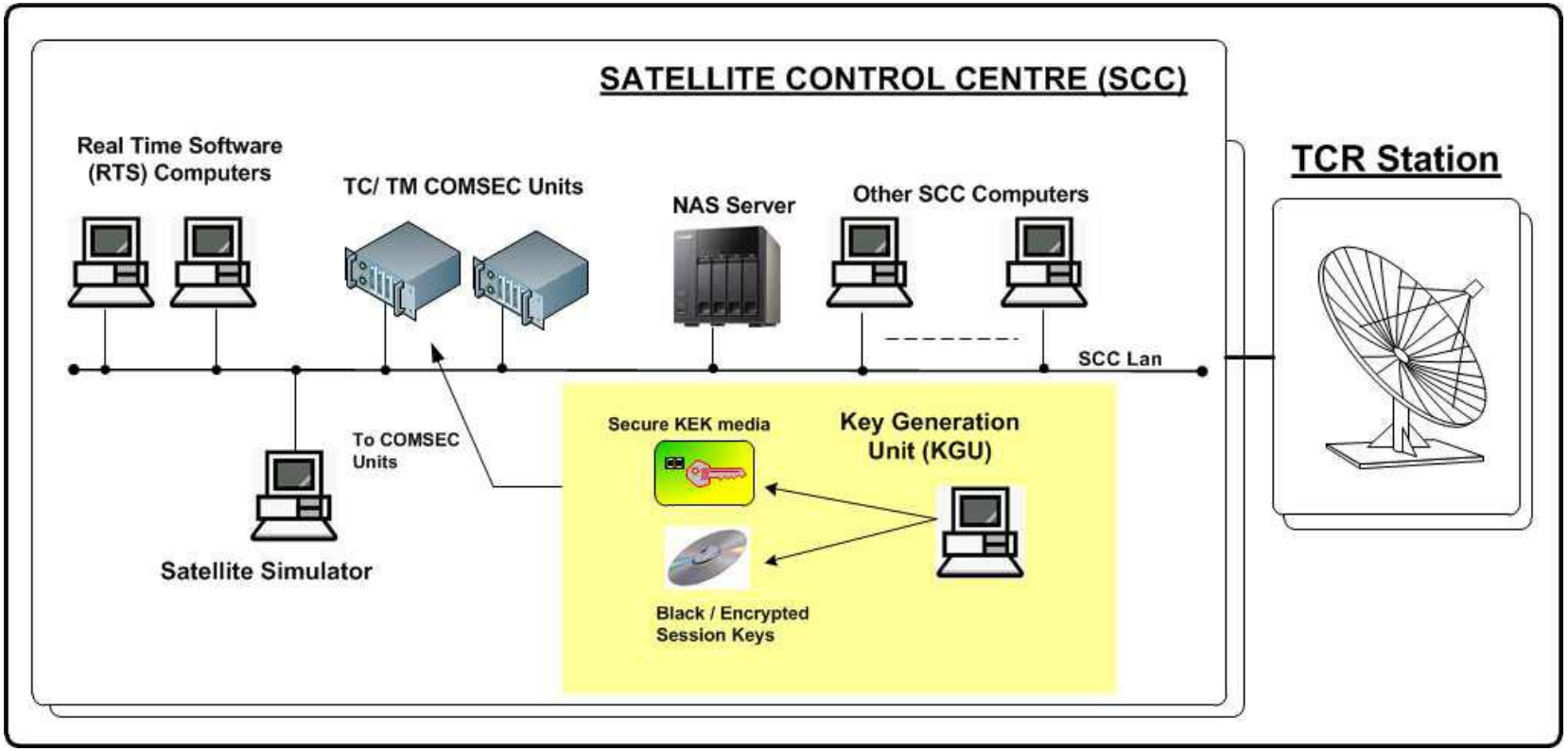
Advanced Encryption Standard (AES) Algorithm Validated Implementations

Validation No.	Vendor	Implementation	Operational Environment	Val. Date	Modes/States/Key sizes/ Description/Notes
3766	AirTight® Networks 339 N. Bernardo Avenue Suite 200 Mountain View, CA 94043 USA -Hemant Chaskar TEL: (650) 961-1111 FAX: (650) 961-1169	**AirTight Sensor Cryptographic Engine** Version 7.2.FIPS.04 (Firmware)	Qualcomm AR9558	12/28/2015	**CBC** (e/d; 128 , 256); **CTR** (int only; 128 , 256) "Implementation performs wireless intrusion detection and prevention. It monitors radio channels to ensure conformance of wireless activity to security policy. It mitigates various types of wireless security violations such as rogue wireless networks, unauthorized wireless connections, network mis-configurations and DoS attacks."
3765	MRV Communications, Inc. 300 Apollo Dr. Chelmsford, MA 01824 USA -Tim Bergeron TEL: 978-674-6860 -Phil Bellino TEL: 978-674-6870	**LX-Series Algorithm Core** Version V6.1.0 (Firmware)	Freescale PQ1 MPC885	12/18/2015	**ECB** (e/d; 128 , 192 , 256); **CBC** (e/d; 128 , 192 , 256); **CFB8** (e/d; 128 , 192 , 256); **CFB128** (e/d; 128 , 192 , 256); **OFB** (e/d; 128 , 192 , 256); **CTR** (ext only; 128 , 192 , 256) "The LX-4000T Series Console Servers provide secure remote service serial port access to devices in an organization"s networks and infrastructures. This nearly eliminates the need for physical presence at a site to correct problems or manage its everyday operation."
3764	MRV Communications, Inc. 300 Apollo Dr. Chelmsford, MA 01824 USA -Tim Bergeron TEL: 978-674-6860 -Phil Bellino TEL: 978-674-6870	**LX-4000T Series IPSec Algorithm Core** Version V6.1.0 (Firmware)	Freescale PQ1 MPC885	12/18/2015	**CBC** (e/d; 128 , 192 , 256); "The LX-4000T Series Console Servers provide secure remote service serial port access to devices in an organization"s networks and infrastructures. This nearly eliminates the need for physical presence at a site to correct problems or manage its everyday operation."
3763	Broadcom Corporation 3151 Zanker Road San Jose, CA 95134 USA -Gary Goodman TEL: 408-922-1092 FAX: 408-922-1023	**SMAU Generic Crypto - CCM** Version 1.0 (Firmware) Part # BCM5810X B0	ARM M3	12/18/2015	**CCM (KS: 128) (Assoc. Data Len Range**: 1 - 32) **(Payload Length Range**: 16 - 32 (**Nonce Length(s)**: 7 8 9 10 11 12 **(Tag Length(s)**: 4 8 12 16) AES Val#3762 "AES CCM implementation with key length of 128 bit"

❑ Exemple 1 : Système TC COMSEC => Gestion des Clés



❑ Exemple 1 : Système TC COMSEC => Gestion des Clés



❑ Exemple 1 : Système TC COMSEC => Gestion des Clés

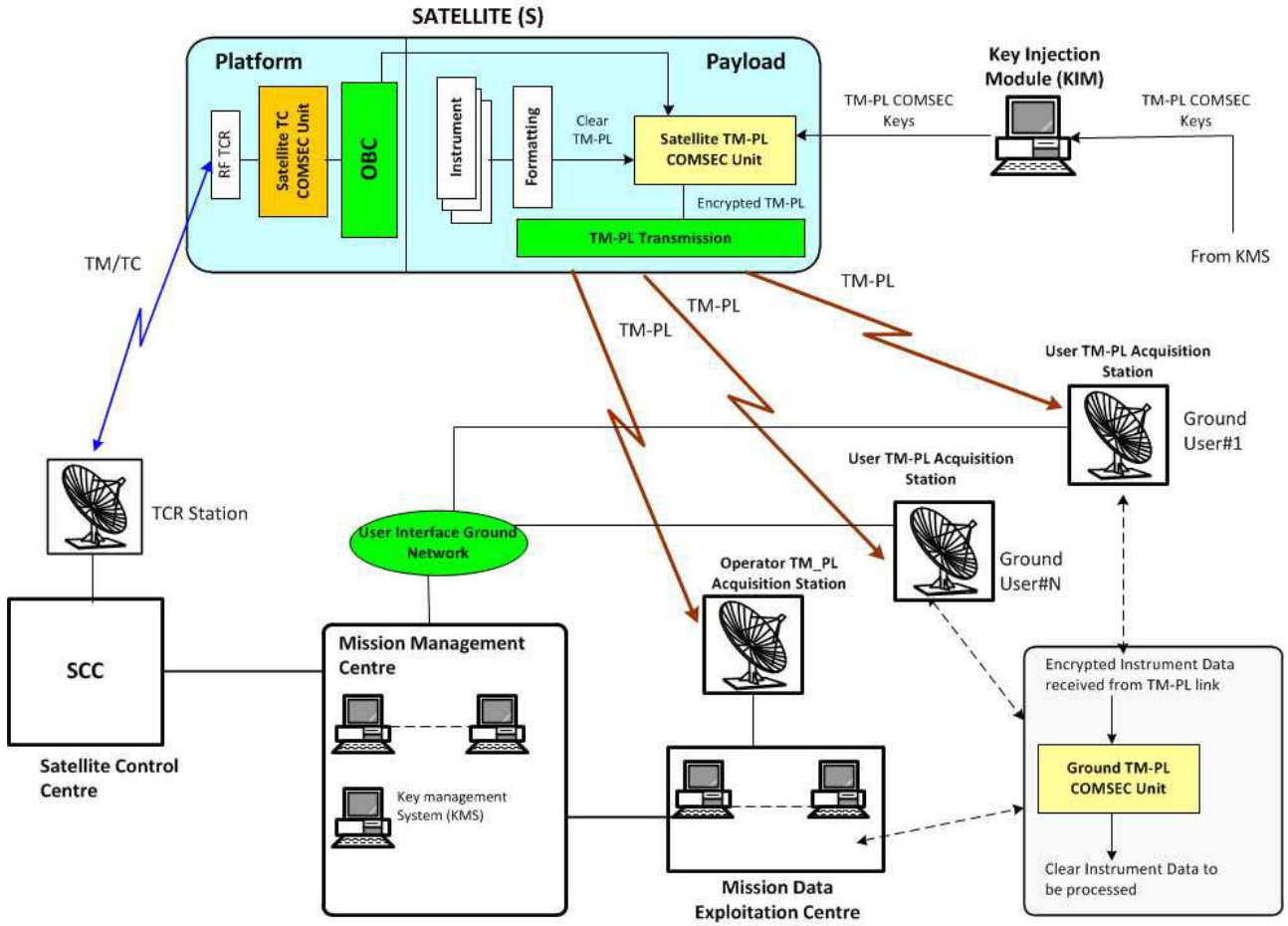
- L'un des points délicats est la génération des clés de vol
  - Pattern de clé aléatoires et non déterministes garantissant leur confidentialité
- Sélection d'un générateur PRNG robuste et standard
  - Ex: le standard NIST SP800-90A spécifie 3 * générateurs pseudo aléatoires utilisant un DRBG (Deterministic Random Bit Generator)
    - HASH_DRBG : basé sur fonctions HASH (SHA_xxx)
    - HMAC_DRBG : basé sur algorithme HMAC-SHAxxx
    - CTR_DRBG : basé sur algorithme CTR-AES
  - Note : le dernier générateur EC_DRBG basé sur des courbes elliptiques a été retiré par le NIST, car fortement mis en cause et en doute par la communauté des experts en cryptographie
- L'élément critique est la source d'entropie
  - Source logicielle : bruit dans le noyau Unix **(/dev/random ou dev/urandom**), compilation (random pool) des divers evènements materiels / logiciels captables par l'OS (souris, clavier, écran, E/S, acces disques, heure, ..)
  - Source matérielle : générateur hardware (modules USB) , générateur DRNG intégré dans les circuits INTEL (i5 / i7)

- La cryptographie peut suivant le Client ou la Mission être imposée

- Exemple : “NSA Approved Cryptography” imposée par le gouvt US
  - Document applicable : CNSSP-12 Information Assurance

- Impose
  - l’implémentation d’équipements COMSEC certifies par la NSA et fabriques par des industriels US agréés
  - La génération des clés par la NSA
  - Des contraintes de sécurité très fortes : ex eqts de sécurité COMSEC surveilles 24/24 par des gardes US agrées lorsque ceux-ci sont transférés hors des USA

❑ Exemple 2 : Système TM-PL COMSEC



❑ Exemple 2 : Système TM-PL COMSEC

➢ Composants Sol

- Key Management System : génération et distribution des clés (Clés de Traffic, KEK)
- Ground TM-PL COMSEC Unit : Déchiffrement et authentification des Trames TM-PL
- Key Injection Module : chargement des clés dans le satellite

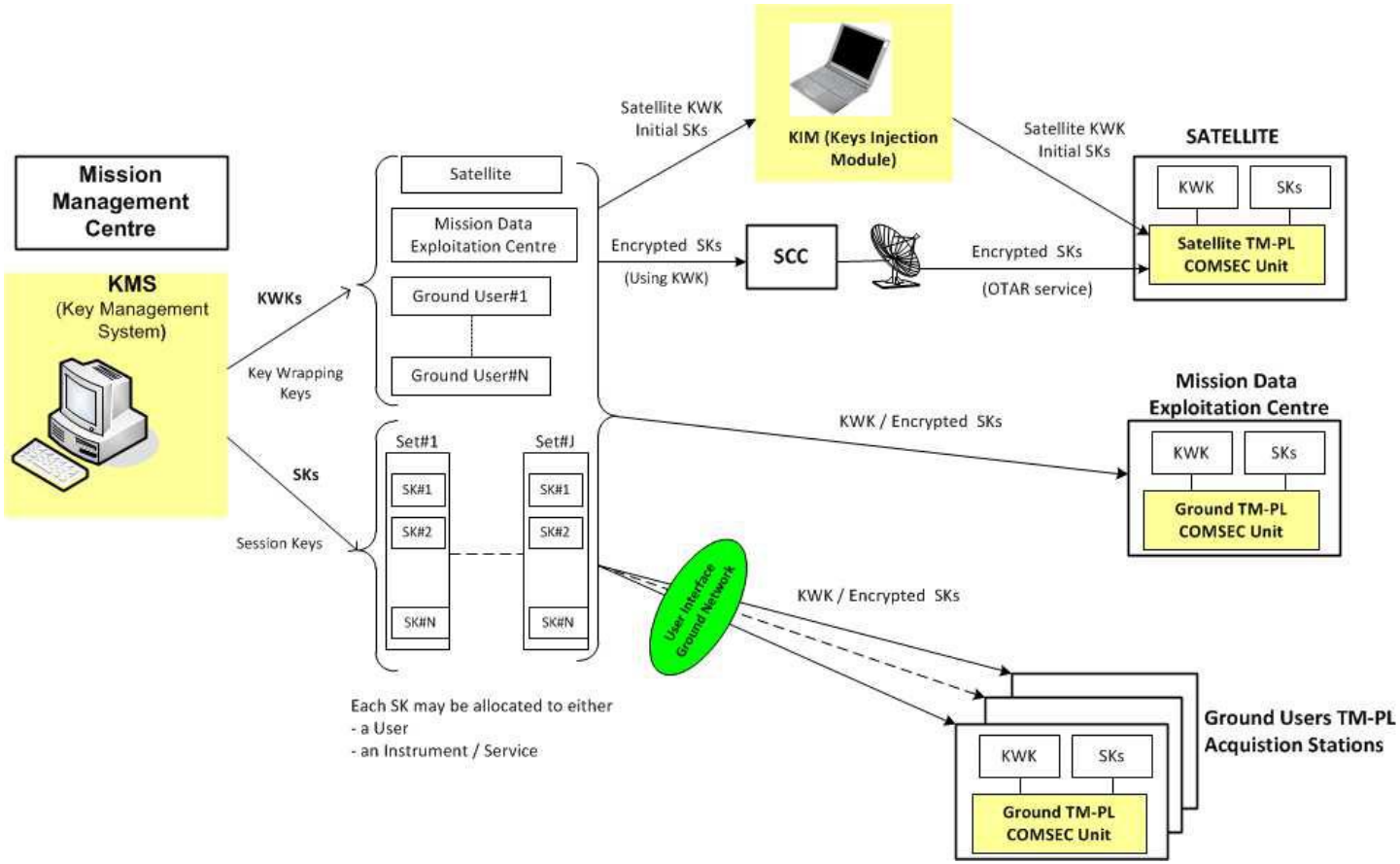
➢ Composants bord / satellite

- Satellite TM-PL COMSEC Unit : chiffrement et authentification des Trames TM-PL

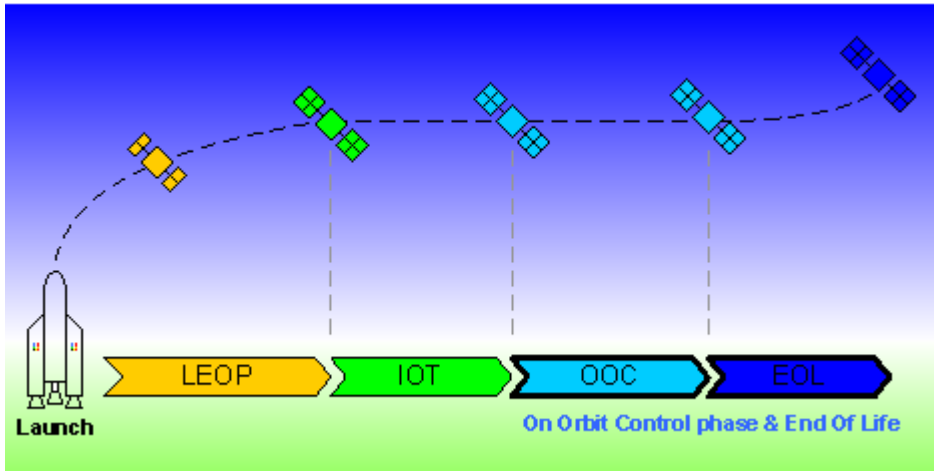
➢ La gestion des Clés est le point le plus delicat d'un système TM-PL COMSEC

- Distribution des Produits instruments : jusqu'à 1000 utilisateurs Sol
- La Gestion des clés TM-PL COMSEC doit obéir à des contraintes de nature dynamique (enregistrement d'un Utilisateur, début / fin du service, révocation)
- La distribution d'un produit Instrument,est très diverse et impacte la Gestion des Clés
  - Broadcast : accès à tous les utilisateurs enregistrés et autorisés
  - Multicast : accès à un sous-ensemble des utilisateurs enregistrés et autorisés
  - Unicast : accès à un seul utilisateur enregistré et autorisé (ex demande prise de vue images au-dessus d'une région donnée)

❑ Exemple 2 : Système TM-PL COMSEC => Gestion des Clés



- Opération d'un système COMSEC/ TRANSEC



- Avant le tir : campagne de tir
  - Chargement des clés de Vol dans le satellite (injection des cles)
- Tir et LEOP phase (Launch & Early Orbit Phase)
  - Pas d'opération sécurité
  - les fonctions de sécurité sont désactivées – Mode "Clair"

- Opération d'un système COMSEC/ TRANSEC

- IOT : In-Orbit-Test
  - Validation du système en Vol
  - Test des fonctions de sécurite à partir du Sol (SCC)

- OOC : Orbit Control Phase : Phase d'exploitation du satellite
  - Initialisation Sécurité
    - Activation des fonctions de Sécurite
    - Initialisation des paramètres: compteur anti-rejeu, clé courante
  - Operation nominale
    - Changement périodique de clé courante
    - Génération et téléchargement de nouveaux jeux de clés (clés fraiches) - OTAR
  - Opérations non nominales
    - Investigations sur pannes, reset, switch sur la redondance, ..

Opération d'un système COMSEC/ TRANSEC

Changement Périodique de Clé

	1rst Month	2nd Month		11th Month	12th Month
1st Year	key#17	key#18	…	key#26	key#28
2nd Year	key#29	key#30	…	key#38	key#40
3rd Year	key#41	key#42	…	key#50	key#52
4th Year	key#53	key#54	…	key#62	key#64
5th Year	key#65	key#66	…	key#74	key#76
6th Year	key#77	key#78	…	key#86	key#88
7th Year	key#89	key#90	…	key#98	key#100
8th Year	key#101	key#102	…	key#110	key#112
9th Year	key#113	key#114	…	key#122	key#124
10th Year	key#125	key#126	…	key#134	key#136
11th Year	key#137	key#138	…	key#146	key#148
12th Year	key#149	key#150	…	key#158	key#160
13th Year	key#161	key#162	…	key#170	key#172
14th Year	key#173	key#174	…	key#182	key#184
15th Year	key#185	key#186	…	key#194	key#196
16th Year	key#197	key#198	…	key#207	key#208

9 – Cas de Systèmes TRANSEC pour la protection des liaison spatiales

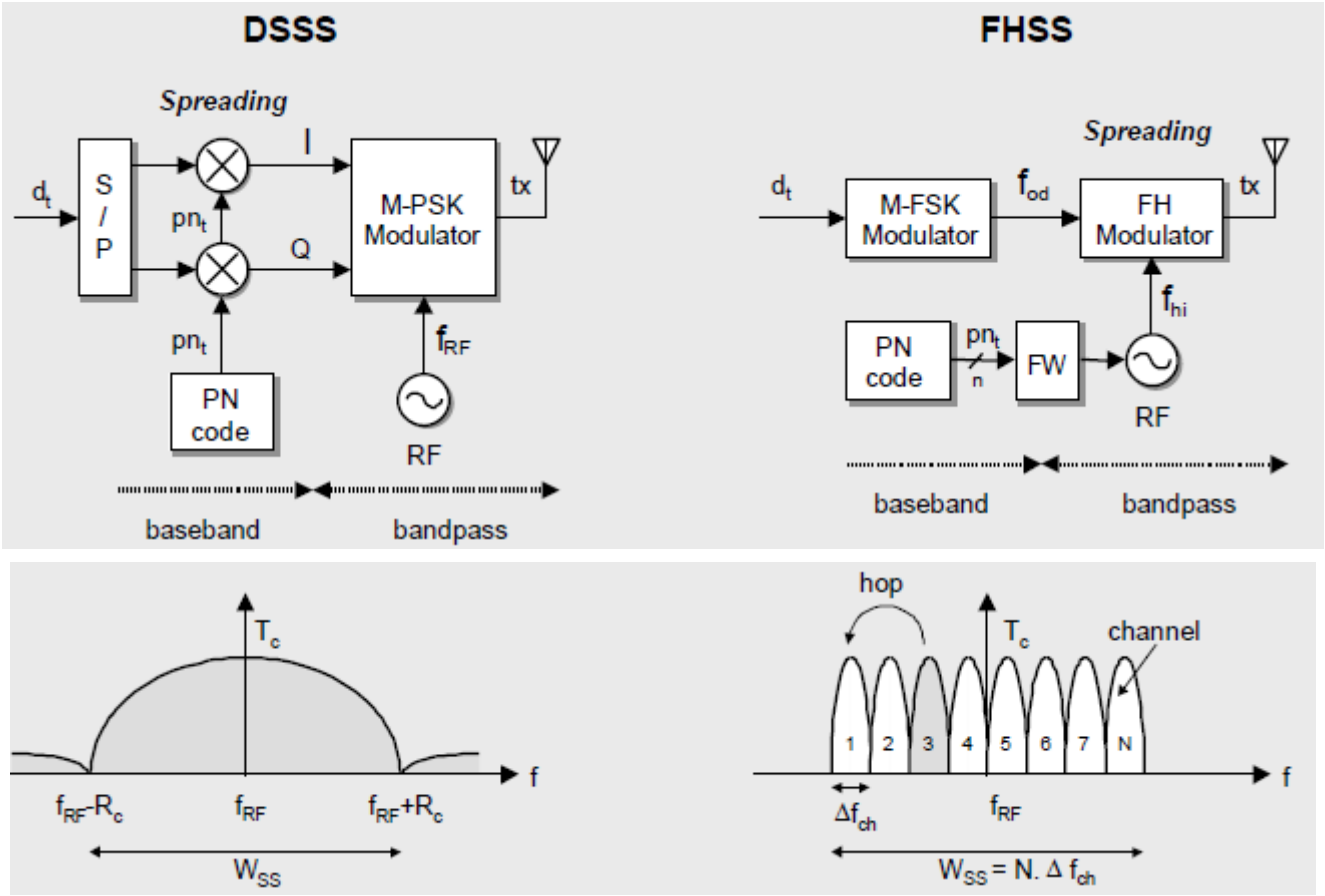
❑ Définition - Un système TRANSEC

- ➢ Assure une protection des données à transmettre contre le brouillage et l'interception
- ➢ Opère au niveau de la couche physique
  - Couche modulation / transmission Radio-Fréquence des données à transmettre
- ➢ Utilise la technologie de Spectre étalé (Spread Spectrum / SS)
  - Direct Sequence : système DSSS
  - Saut de Fréquence (frequency hopping): système FHSS
- ➢ Met en oeuvre des mécanismes cryptographiques
  - Génération des séquences dites TRANSEC pilotant les fonction d'étalement de spectre et assurant leur qualité et confidentialité
- ➢ Affiche des performances (anti-brouillage) compatible des besoins / exigences de niveau Gouvernemental / Défense
  - Principaux utilisateurs des systèmes TRANSEC

Principe d'un système TRANSEC

- Le principe consiste à transforrmer le signal contenant les données utiles à transmettre (signal occupant une bande étroite), en un signal occupant une bande beaucoup plus étendue (large-bande) et semblable à du bruit
  - La bande de fréquence résultante peut-etre 100 à 1000 fois plus étendue que la bande étroite utile nécessaire à la transmission des données d'entrée
- Comme la puissance de transmission du signal large-bande est identique à celle du signal à bande etroite, la densité spectrale du signal (W/Hz) s'en trouve proportionnellement réduite
- Du fait que le signal utile à transmettre est réparti sur bande de fréquence nettement plus large et qu'il est difficilement distinguable du bruit:
  - Il est nettement plus difficile à intercepter => LPI : Low Probability to Intercept
  - Il est nettement plus resistant au brouillage => AF anti-jamming
- Les lois d'étalement de spectre sont basées sur des sequences pseudo-aléatoires dites PN (pseudo Noise) , générées par un algorithme cryptographique (elles deviennent alors des séquences TRANSEC)

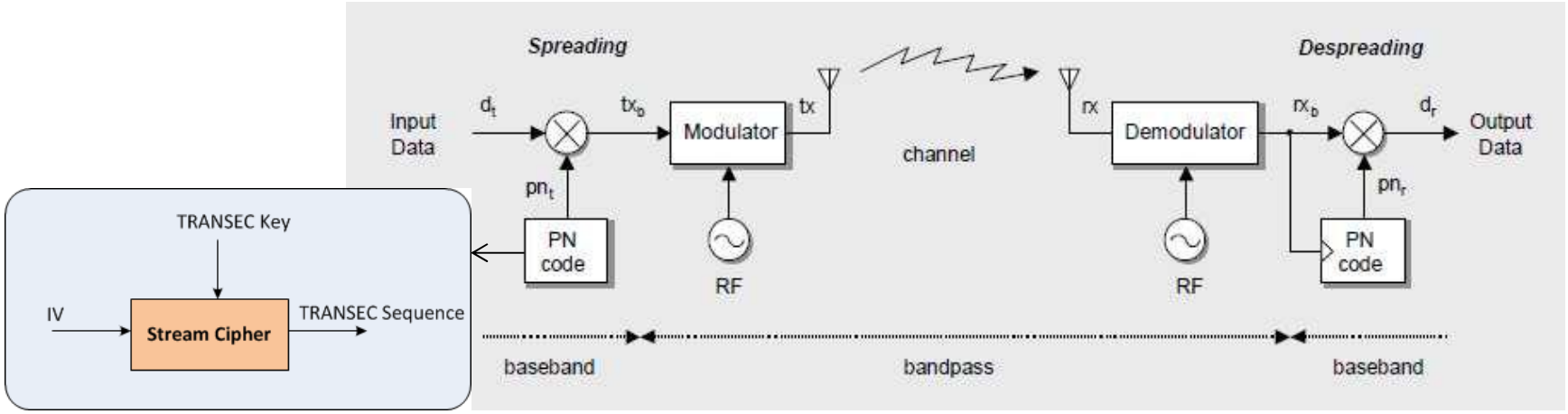
❑ Principe d'un système TRANSEC DSSS et FHSS



Role des fonctions cryptographiques dans un système TRANSEC

Système DSSS

- Génération de la sequence pseudo-aléatoire (PN Code dans la figure) haut-débit additionnée (XOR) avec la séquence utile d'entrée
- Implémentation d'une fonction PRNG (pseudo-random number generator) basée sur un stream cipher et des clés secrètes
  - ex: OFB-AES, CTR-AES, RABBIT, SNOW, SALSA_20

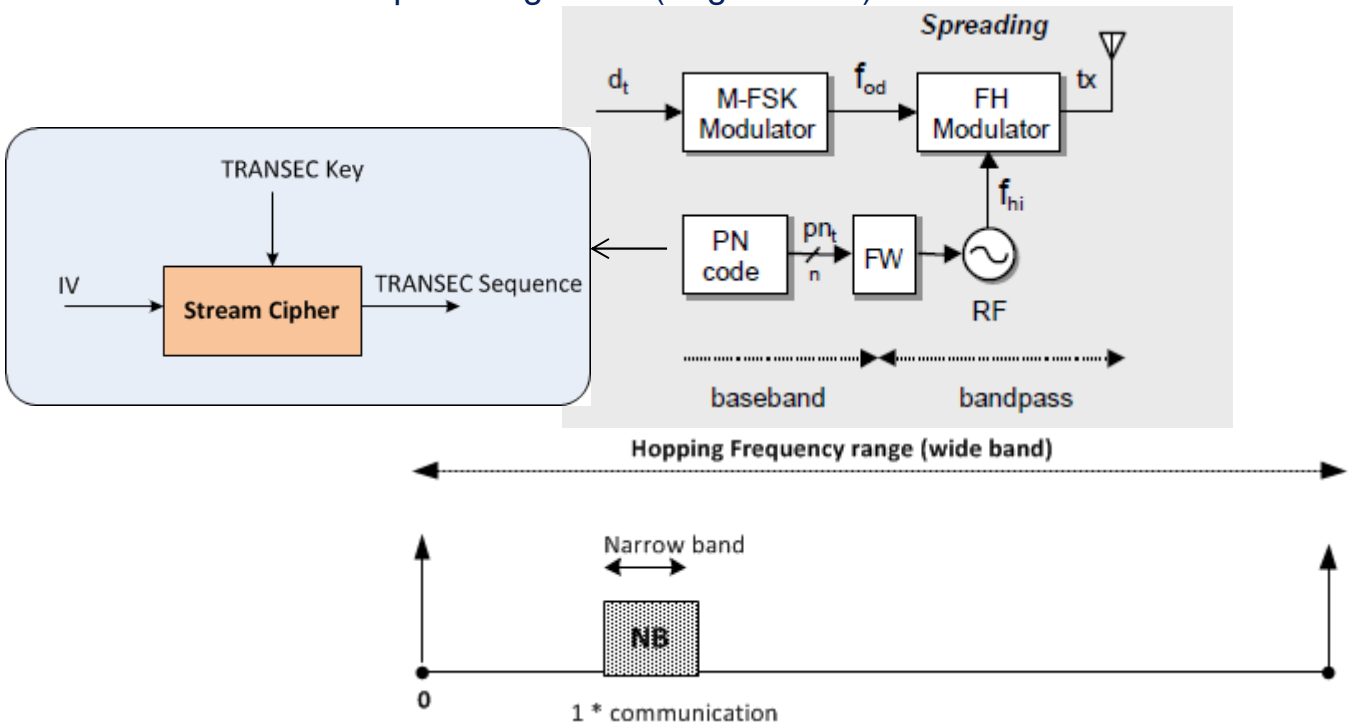


❑ Role des fonctions cryptographiques dans un systéme TRANSEC

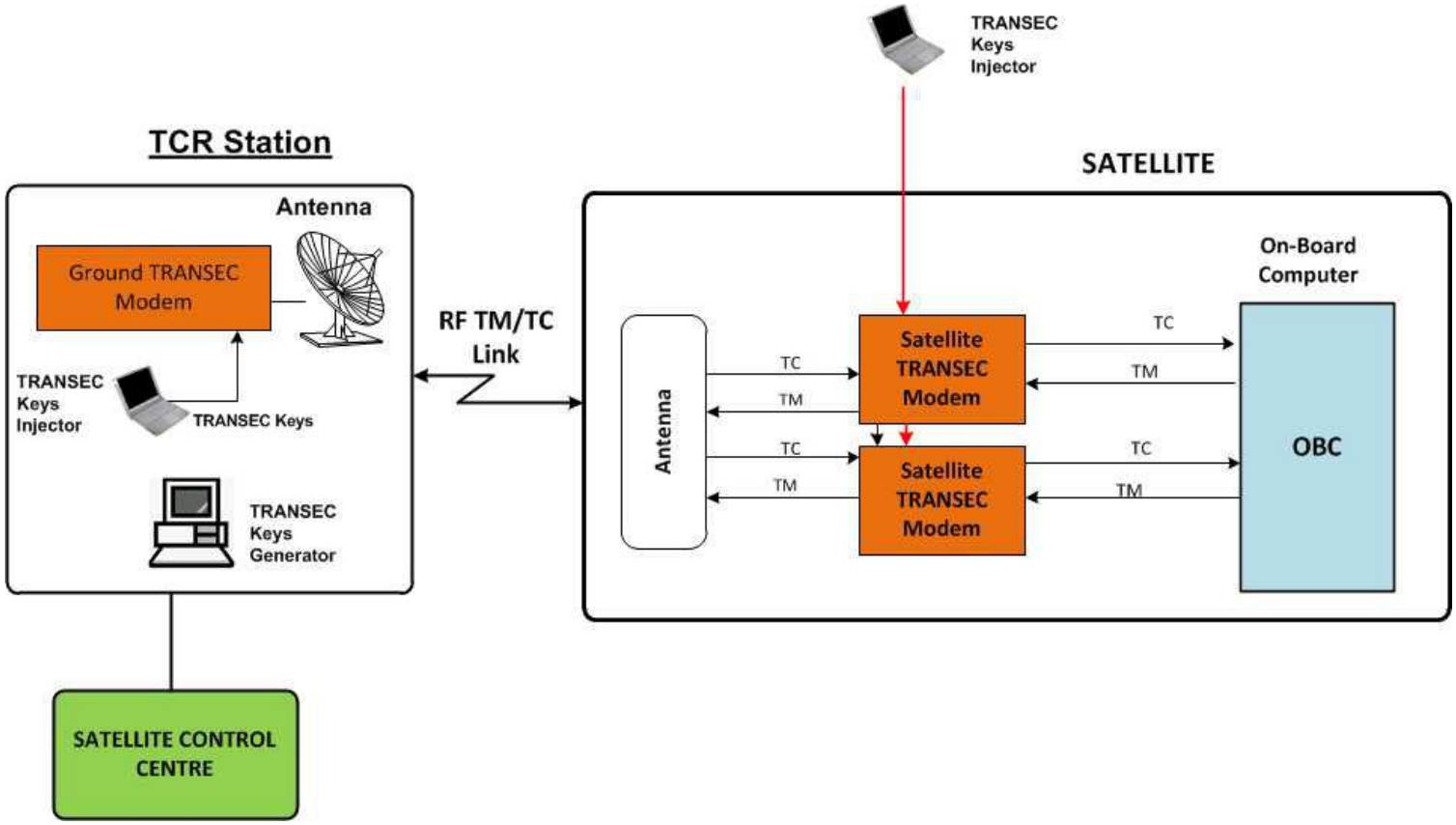
➢ Caractéristique des séquences TRANSEC

- Pseudo aléatoires : doivent paraitre parfaitement aléatoires à ceux qui écoutent le signal RF large bande sans connaître la loi TRANSEC
  - Caractéristiques statistiques : moyenne , écart type, ..
- Déterministes : la loi TRANSEC doit être connue de l'emetteur et du Récepteur (Sol et Satellite)
- Non linéaire
- Longue crypto-période rendant plus difficile l'analyse
  - Typiquement une période superieure à la durée d'une mission spatiale (10 à 20 ans) repond à ce besoin
- Génération par une cryptographie forte
  - algorithme, mode d'opération, taille de clé

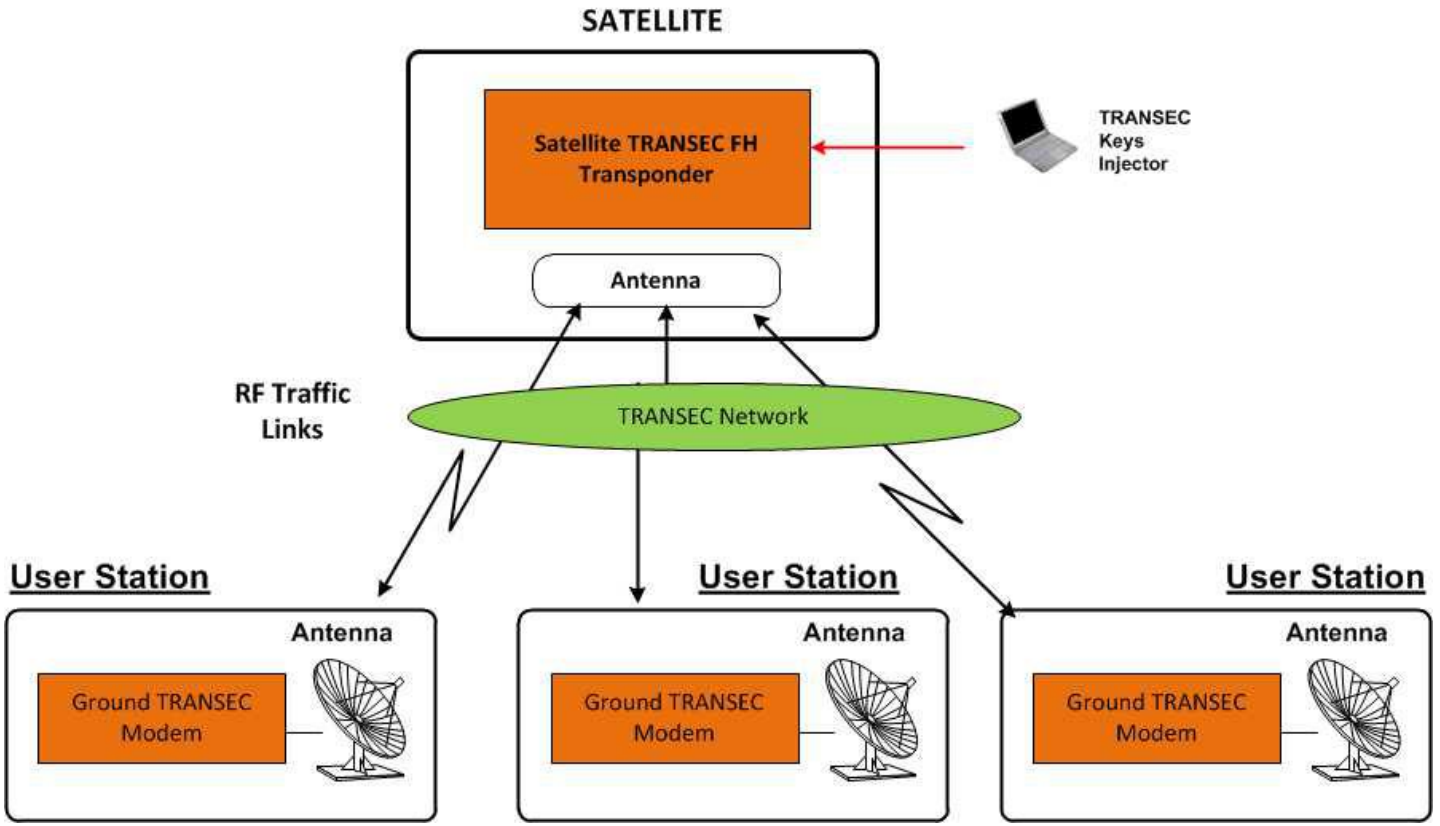
- Role des fonction cryptographiques dans un systéme TRANSEC
  - Système FHSS
    - Génération de la sequence pseudo-aléatoire déterminant la position de la bande de fréquence étroite transportant la communication en cours à l'instant T , dans la bande de fréquence globale (large bande)



❑ Exemple : Configuration d'un Système TRANSEC TC (DSSS)



❑ Exemple : Configuration d'un Système TRANSEC Payload (FHSS)



10 – Conclusion, Discussion

10 – Conclusion

- La sécurité des communications spatiales est un domaine très riche et en permanente évolution
- Exigences en Sécurité accrues des Clients et Opérateur satellites, avec l'accroissement des menaces (Cyber attaques, ordinateurs quantiques)
- Emergence de standards de sécurité (CCSDS) matures pour la protection des liaisons spatiales
- Met en oeuvre les différentes technologies disponibles et futures en cryptographie (SKI, PKI, cryptographie quantique), cryptographie post quantique
- Les solutions de sécurité impactent les segments sols, les satellites, les interfaces bord / sol
  - Centre de contrôle satellite, réseaux sol, sous-systèmes TM / TC satellite, Data handling satellite (Avionique), Charge utile satellite
- De ce fait les Ingénieurs Sécurité sont impliqués aussi bien dans les architectures Sol que les architectures satellites
- Bref , métier passionnant , je conseille….

Fin de la Presentation

ENAC
TLS-SEC
Sécurisation des Communications Drones

Jean-Christophe Schiel

DEFENCE AND SPACE

Jean-Christophe.Schiel@airbus.com

AIRBUS

Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

Sommaire

Introduction

- Les systèmes de communication dans les UAVs:

- **Liaisons de données**
  - Transmission de données nécessaires au fonctionnement du drone: télécommandes et télémesures
  - Transmission vers un centre d'exploitation des données recueillies pendant la mission

    USAGE PRINCIPAL

- **Charges utiles**
  - Fourniture sur une zone ou théâtre d'opérations, d'un service de communication (routeur, point d'accès …)
  - Relais radio dans le but d'augmenter la portée ou résoudre les problèmes d'inter-visibilité d'un système de drone

    USAGES MILITAIRES & SECURITE CIVILE

Introduction

- Types de liaisons de données:

- **LOS (Line Of Sight) : Utilisable quand les conditions de visibilité radio sont établies. Caractérisé par:**
  - Très haut débit, jusqu'à 300Mbps
  - Portées jusqu'à 300 km
  - Discrétion et résistance au brouillage

- **BLOS (Below Line Of Sight): Utilisation d'un relais par satellite. Caractérisé par:**
  - Portée quasi-illimitée
  - Débit limité à quelques Mbps(sauf optique)
  - Faible discrétion et forte sensibilité au brouillage
  - Dépendance des opérateurs civils

Introduction

- LOS vs BLOS:

- **LOS et BLOS (relais satellite radio) régis par les mêmes lois. Quelques spécificités:**
  - BLOS -Satellite:
    - Propagation quasi «espace libre»
    - Pointage de l'antenne embarquée critique pour se conformer aux prescriptions de l'opérateur
  - LOS:
    - Nécessite pour la propagation la prise en compte de l'atmosphère et de la proximité de la terre -> distorsions possibles du canal qui doivent être compensées

Introduction

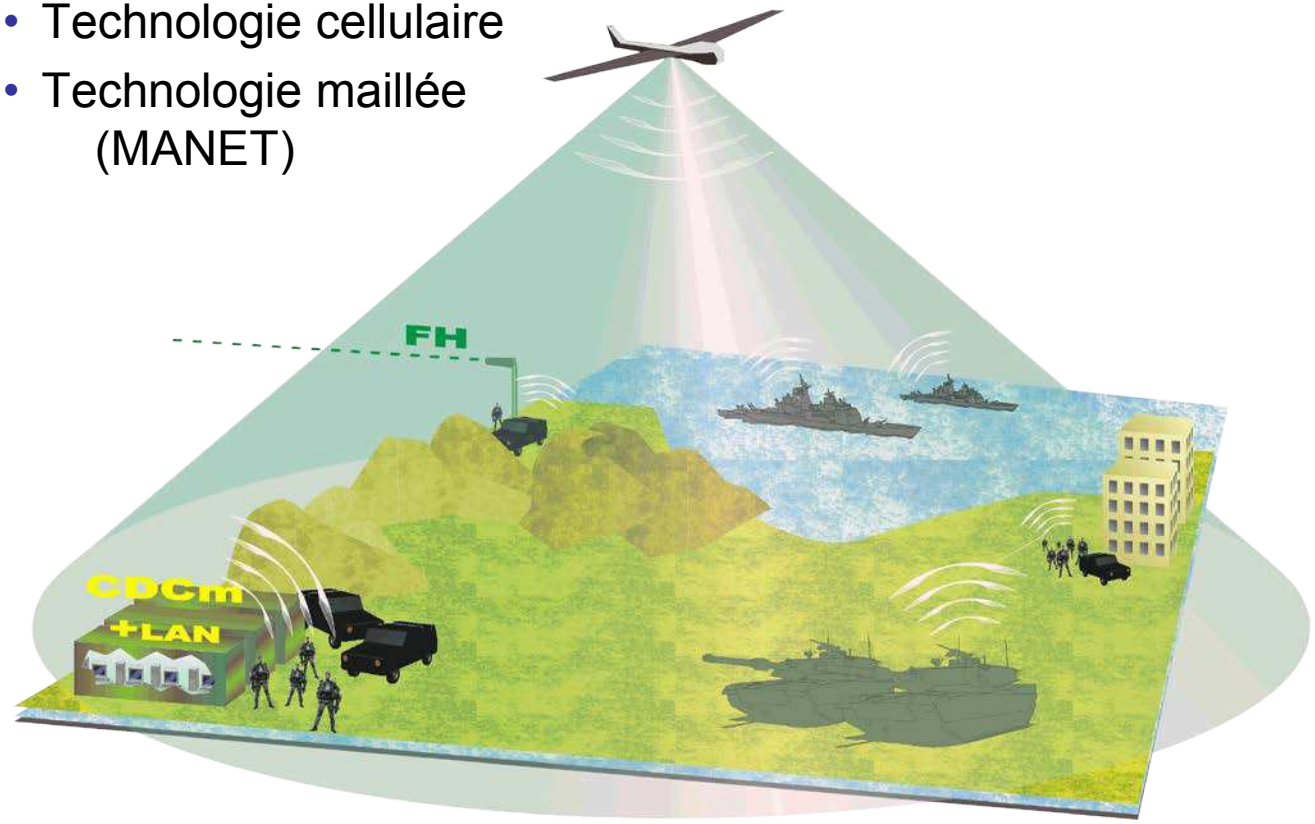
- Pourquoi une liaison de donnée:

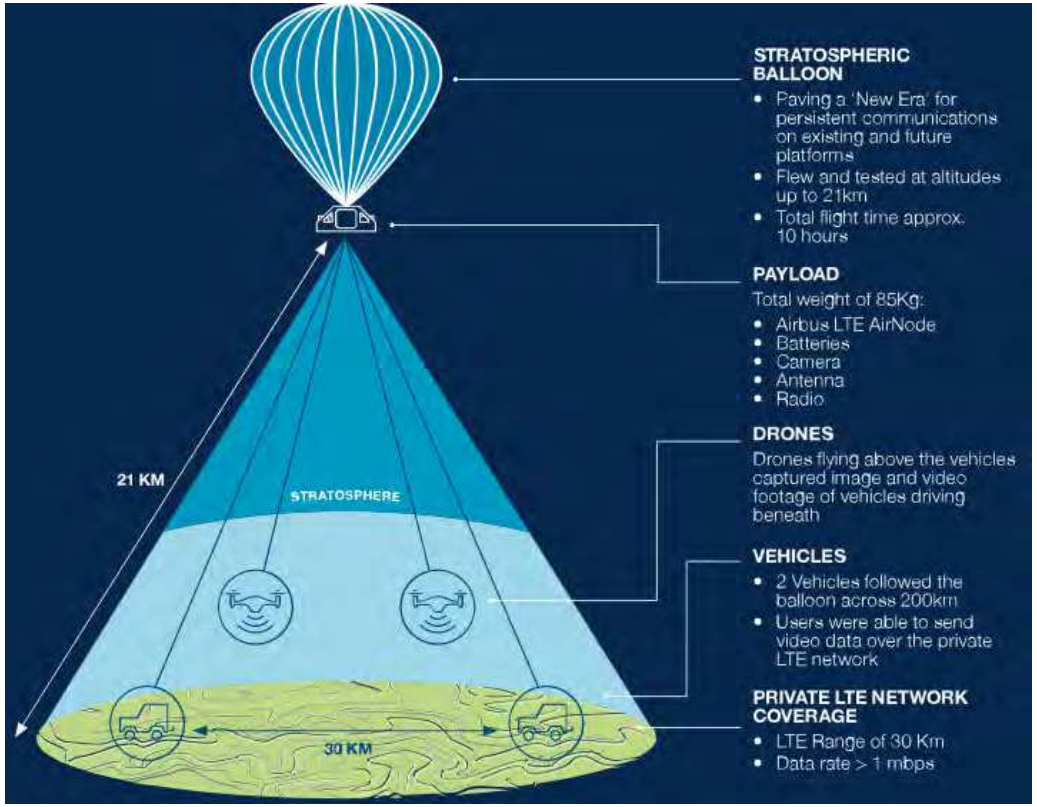
- **Fonction de « transmission »**
  - Dans le sens montant: Télécommande (TC) de quelques dizaines de kbps
  - Dans le sens descendant:
    - Télémesure (TM) de quelques dizaines de kbps
    - Données de mission de quelques Mbps à quelques dizaines de Mbps

- **Fonction de localisation du drone (LOS uniquement & à usage principalement militaire):**
  - GPS pas systématiquement utilisé
  - Mode «backup» souvent exigé en cas de panne ou d'indisponibilité du GPS

Introduction

- Fonction de communication comme charge utile:
- **« Nœud de communication aéroporté »**
  - Technologie cellulaire
  - Technologie maillée (MANET)

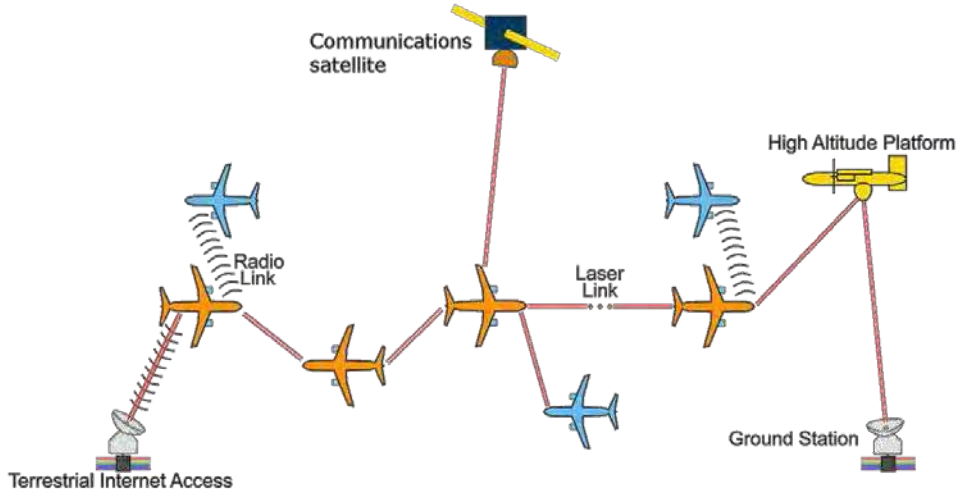


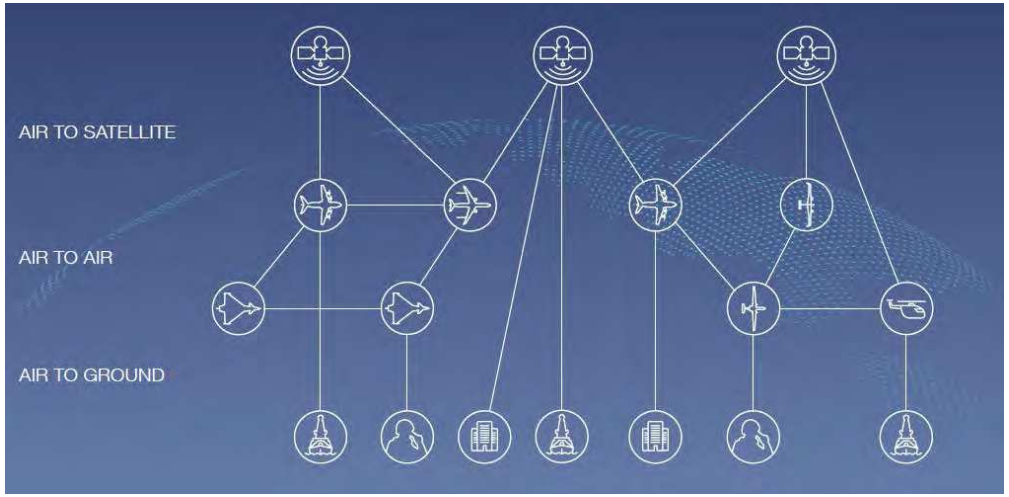


AIRBUS

Introduction

- Fonction de communication comme <u>charge utile</u>:
- **« Nœud de communication aéroporté »**
  - Technologie cellulaire
  - Technologie maillée (MANET)





AIRBUS

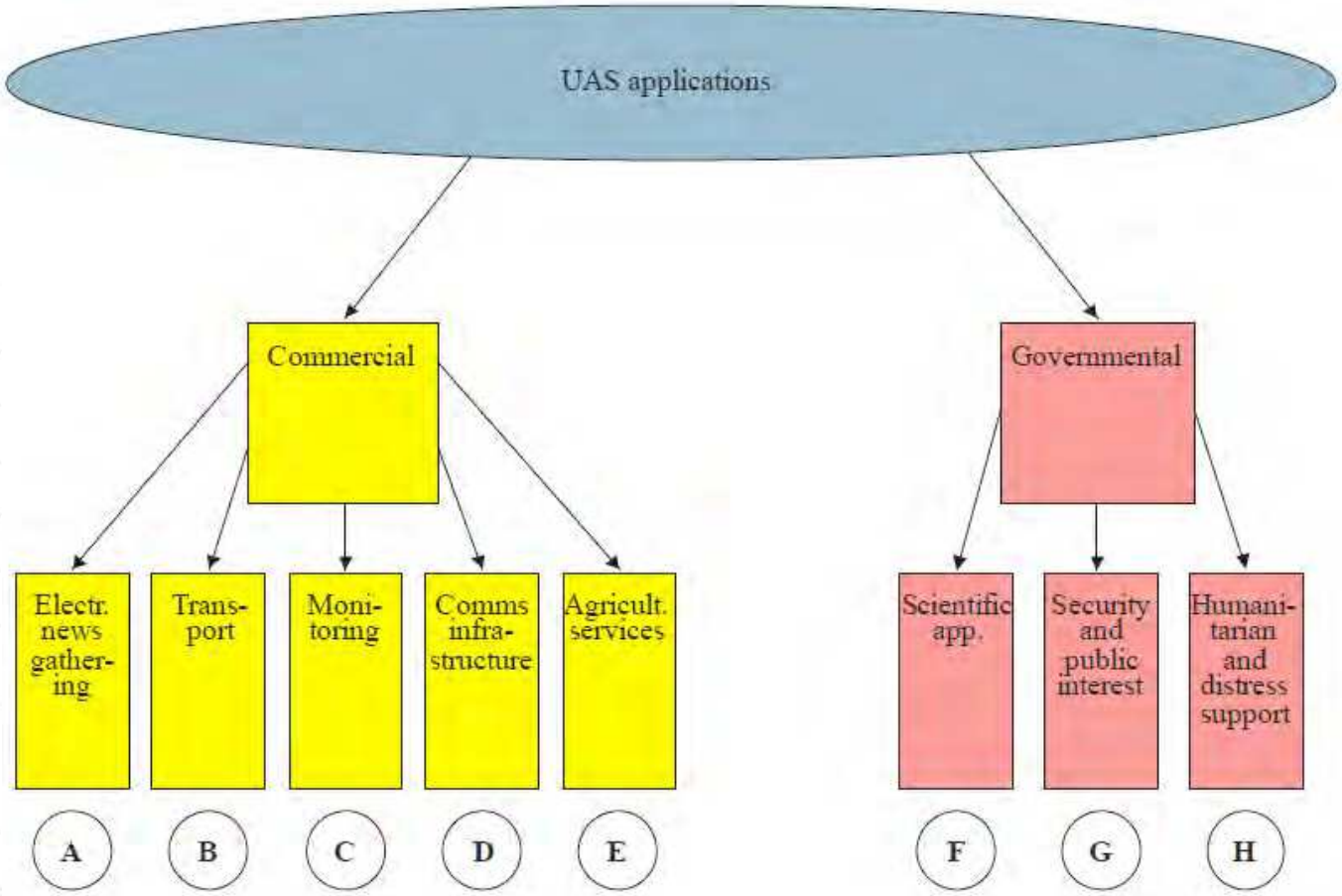
Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

Missions et Technologies

- Missions civiles:

Mission type	Example description
A	Movie making, sports games, popular events like concerts.
B	Cargo planes with reduced man power (one-man-cockpit).
C	Inspections for industries, e.g. oil fields, oil platforms, oil pipelines, power line, rail line.
D	Provision of airborne relays for cell phones in the future.
E	Commercial agricultural services like crop dusting.
F	Earth science and geographic missions (e.g. mapping and surveying, aerial photography) biological, environmental missions (e.g. animal monitoring, crop spraying, volcano monitoring, biomass surveys, livestock monitoring, tree fertilization).
G	Coast line inspection, preventive border surveillance, drug control, anti-terrorism operations, strike events, search and rescue of people in distress, and national security. Public interest missions like remote weather monitoring, avalanche prediction and control, hurricane monitoring, forest fires prevention surveillance, insurance claims during disasters and traffic surveillance.
H	Famine relief, medical support, aid delivery. Search and rescue activities.

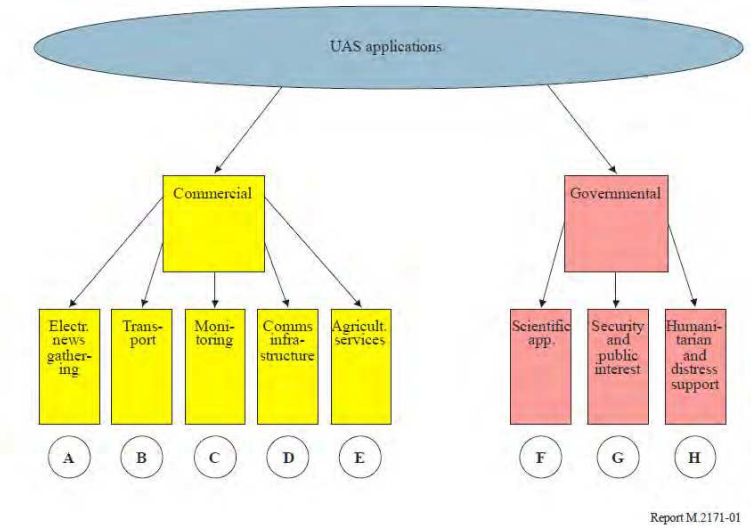


Report M.2171-01

AIRBUS

Missions et Technologies

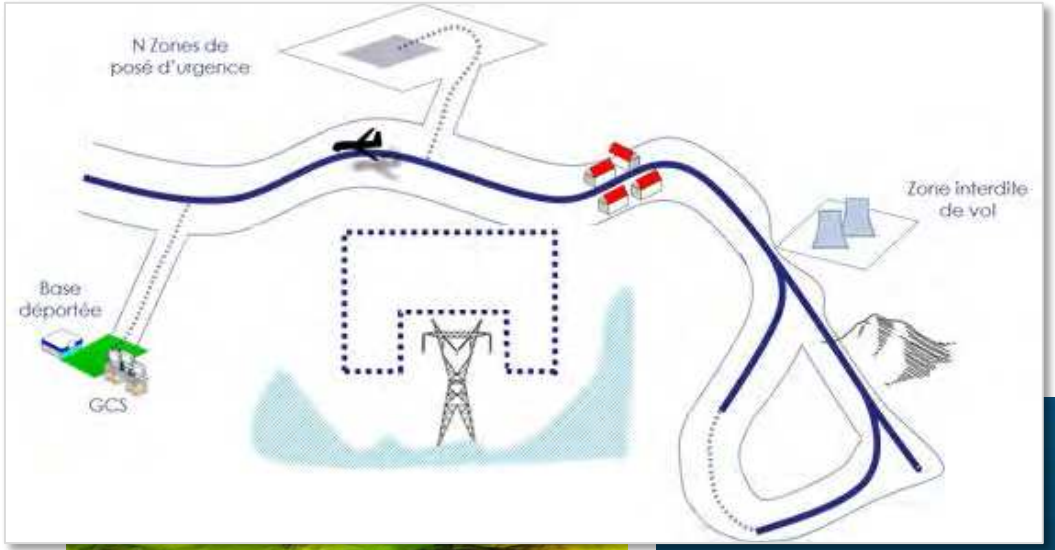
- Missions civiles:

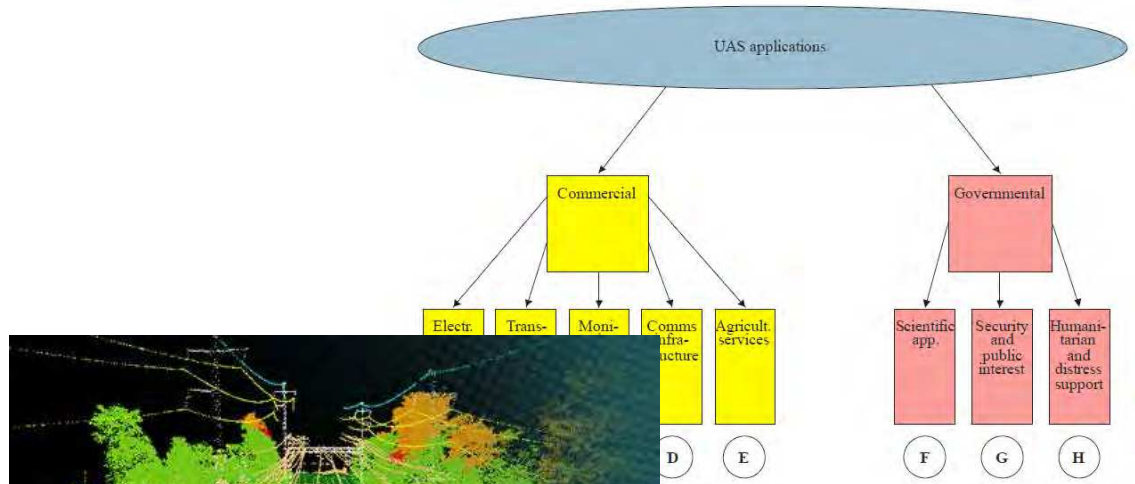


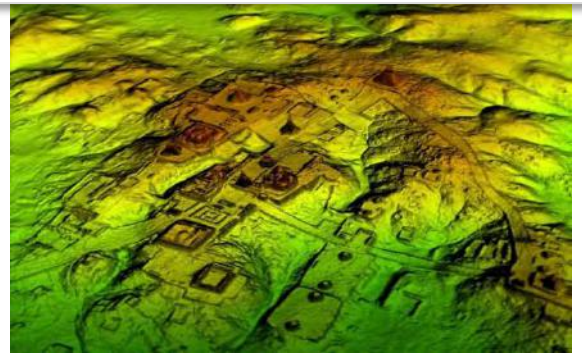
AIRBUS

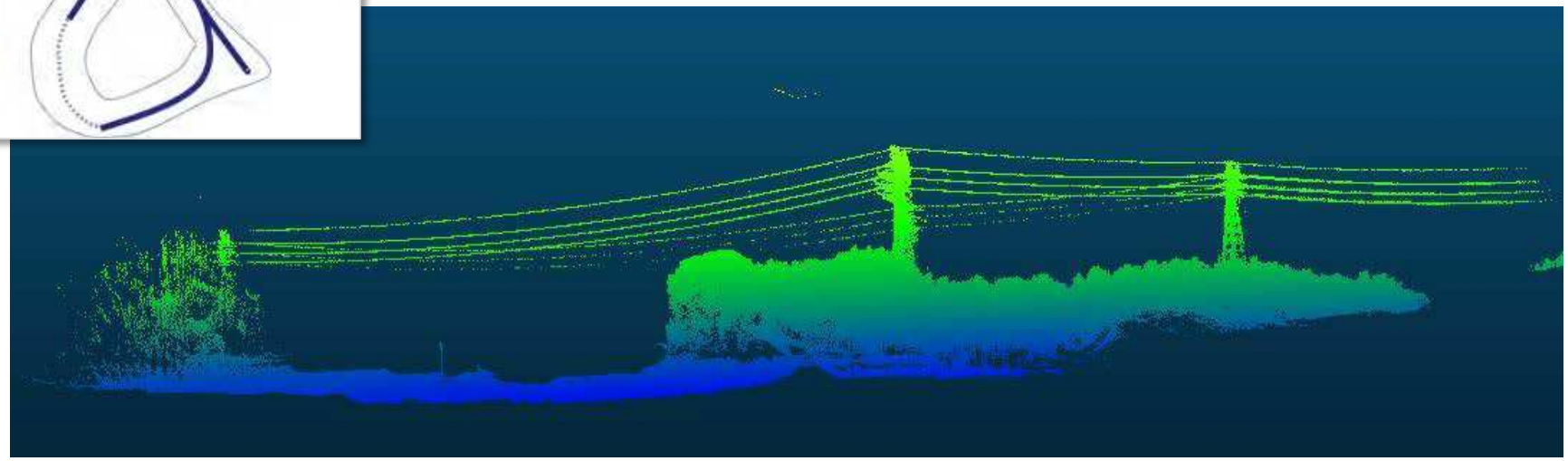
Missions et Technologies

- Missions civiles: grande élongation





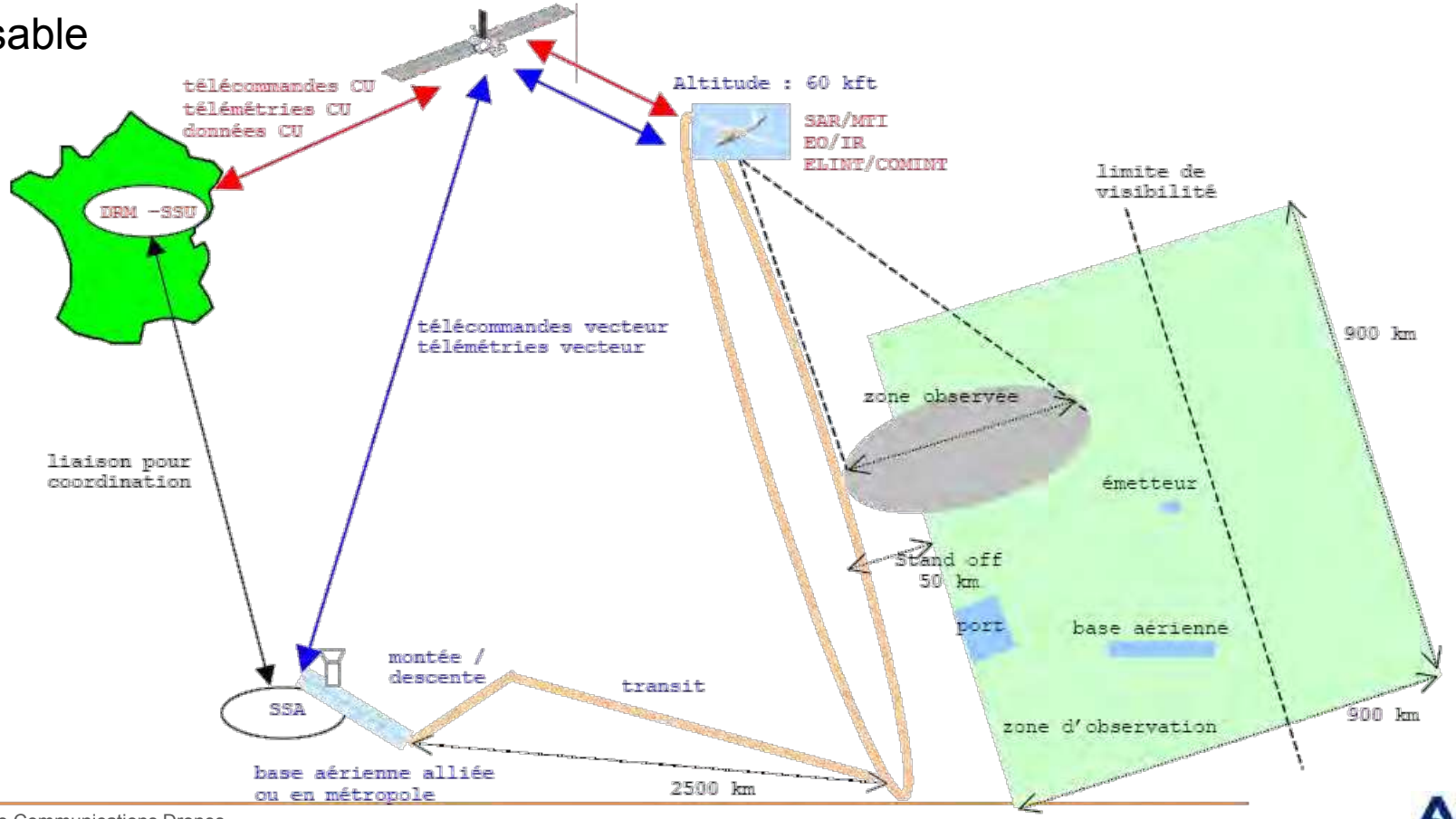




AIRBUS

Missions et Technologies

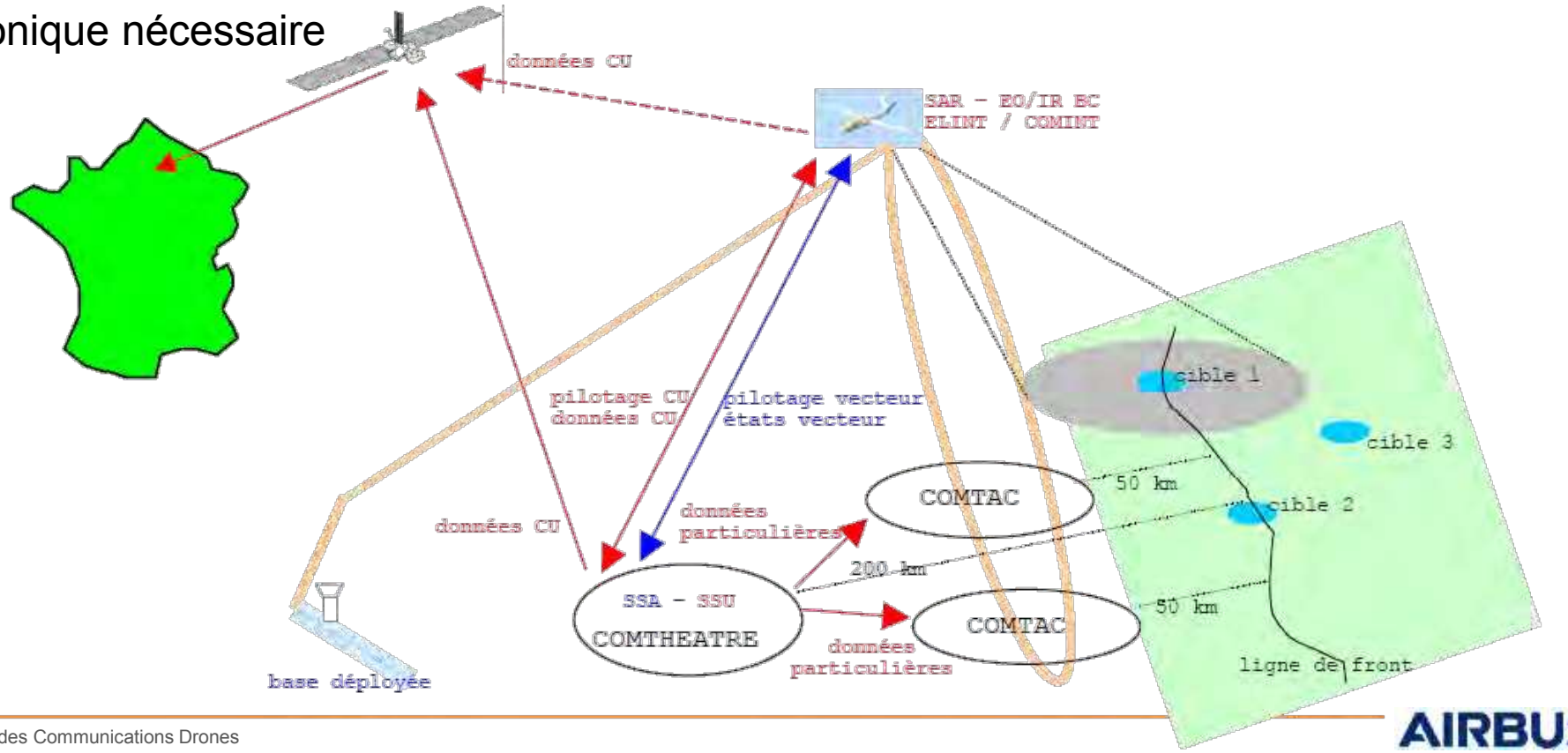
- Missions militaires:
- **Surveillance de zone étendue <u>en temps de paix ou de pré-crise</u>:**
  - Temps réel non indispensable
  - LOS facultative



AIRBUS

Missions et Technologies

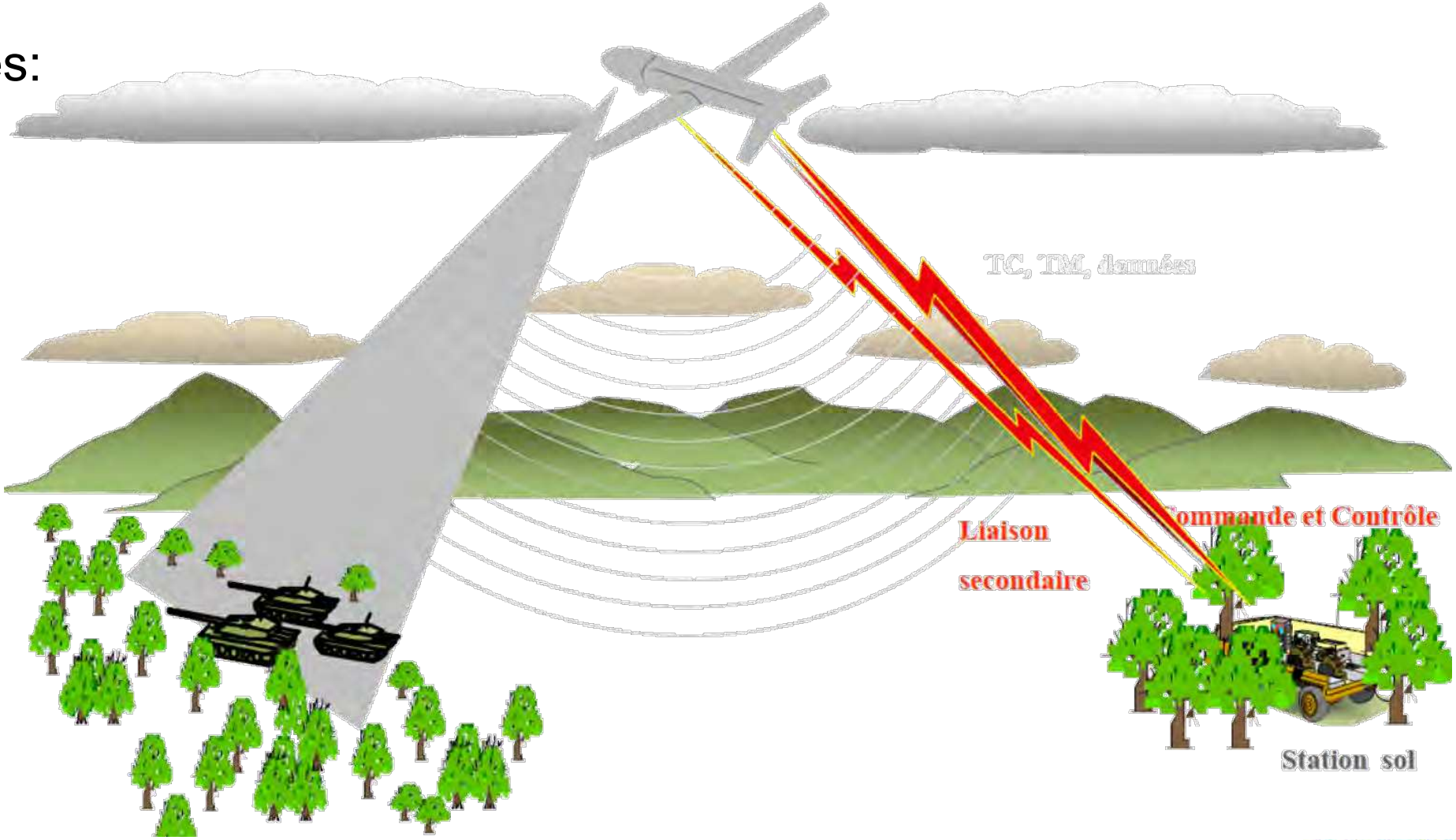
- Missions militaires:
- **Surveillance de zone étendue en temps de crise ou de conflit:**
  - Temps réel et haut débit indispensables (Time Sensitive Targets)
  - Protection guerre électronique nécessaire
  - LOS indispensable



AIRBUS

Missions et Technologies

- Missions militaires:



AIRBUS

Missions et Technologies

Partie Sol
GDT (LOS)

- Missions militaires: exemples

AIRBUS

Missions et Technologies

Partie Bord
ADT (LOS)

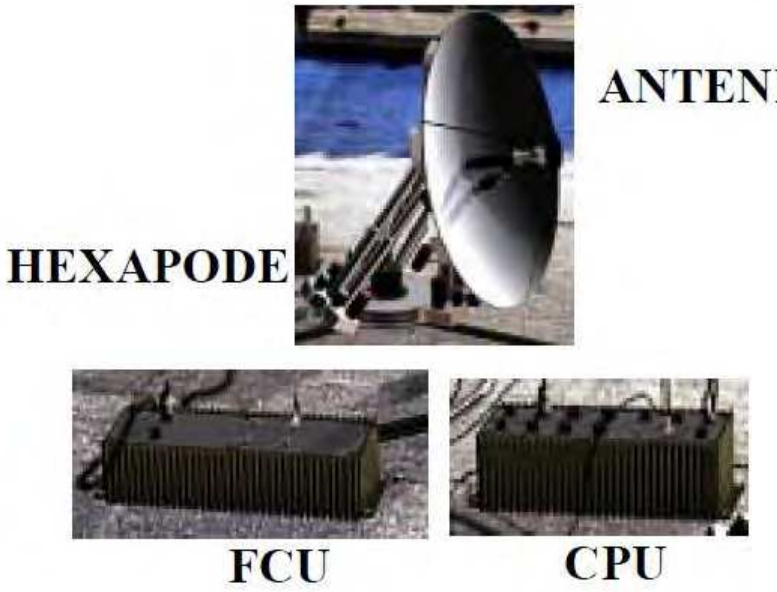
- Missions militaires: exemples
  Harfang

AIRBUS

Missions et Technologies

Partie Bord Satcom (BLOS)

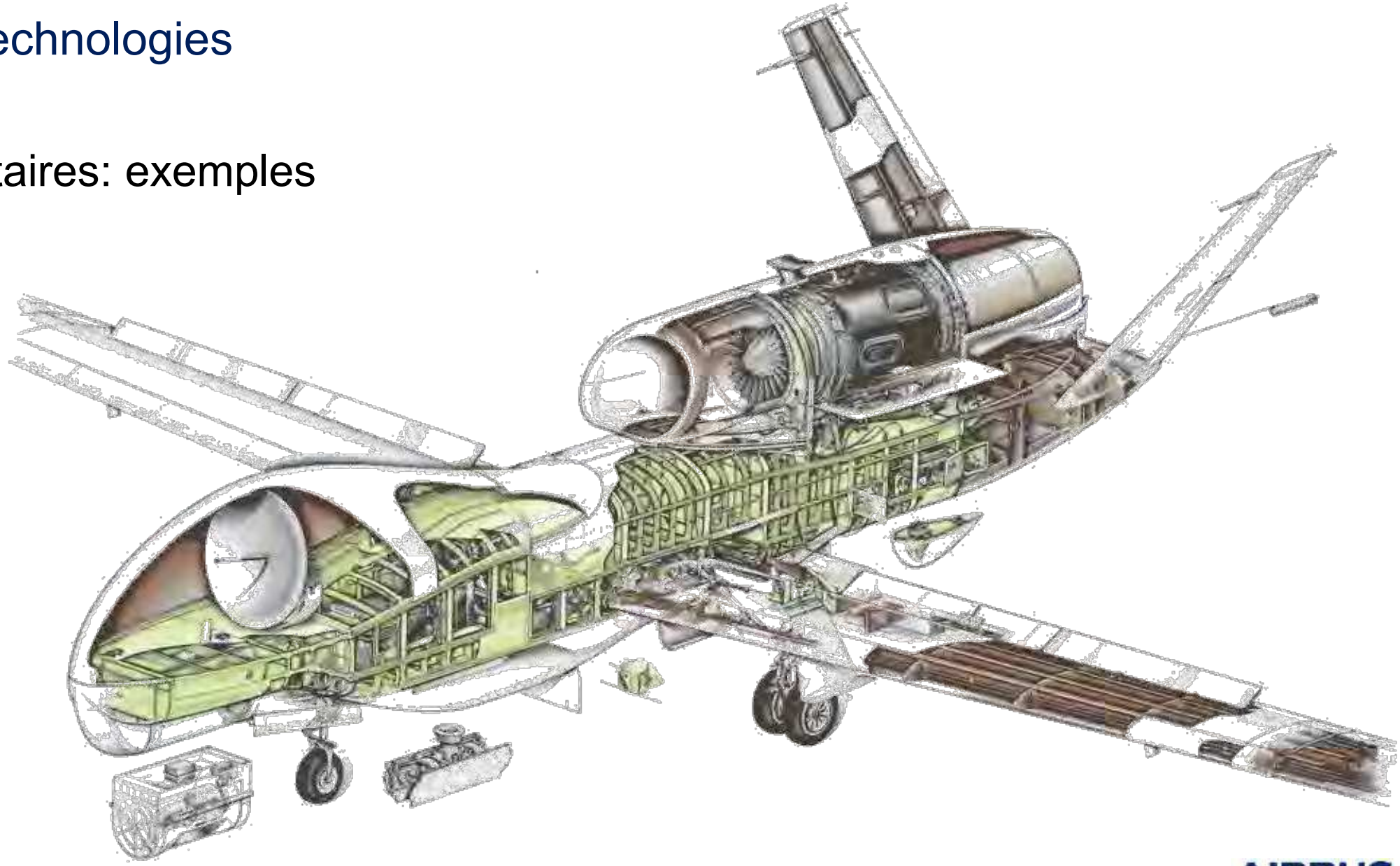
- Missions militaires: exemples
  Harfang



AIRBUS

Missions et Technologies

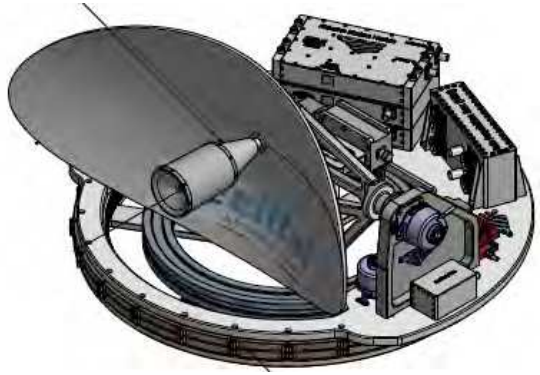
- Missions militaires: exemples



AIRBUS

Missions et Technologies

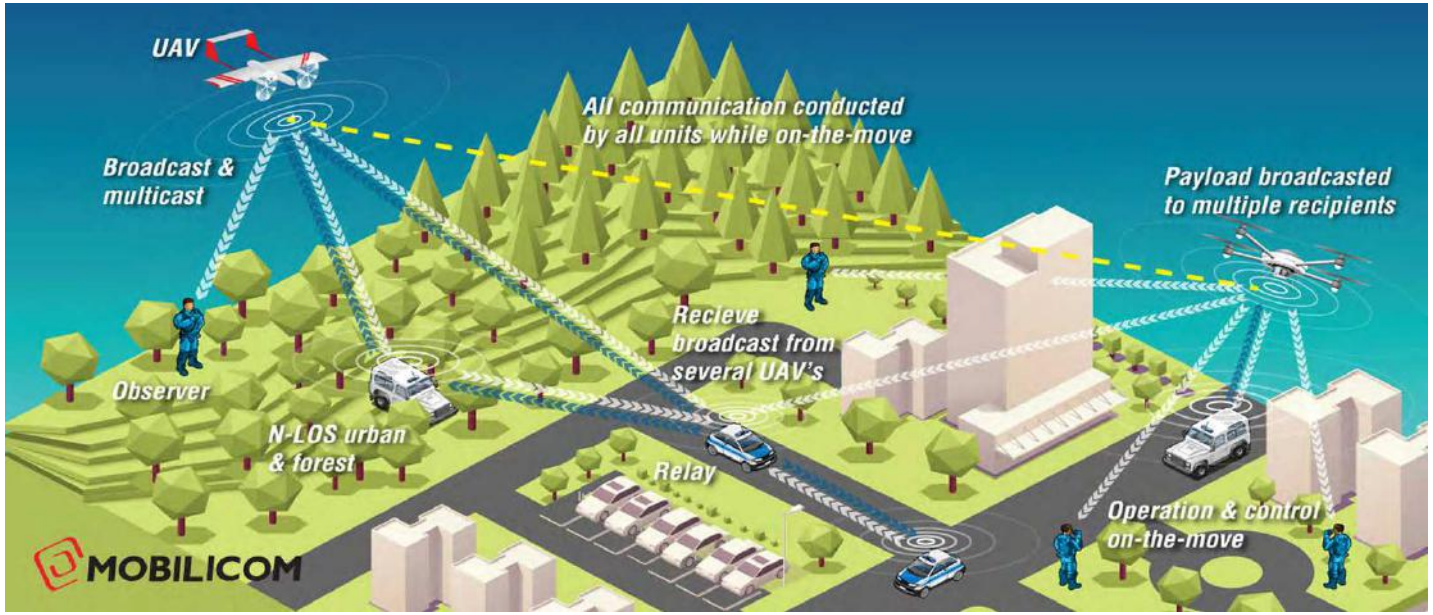
- Technologies:
  - Communications drones ?
    - BLOS: Relais via satellite

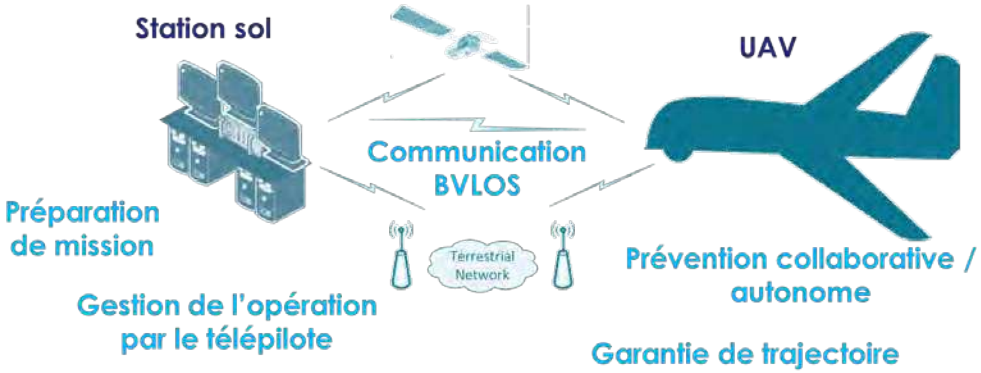


    - LOS: Relais via station dédiée au sol
    - *LOS: Relais via réseau dédié au sol / aérien*
    - *LOS: Relais via réseaux des opérateurs mobiles*

Missions et Technologies

- Technologies:
  - Communications drones ?
    - LOS: Relais via réseau dédié au sol / aérien
    - LOS: Relais via réseaux des opérateurs mobiles





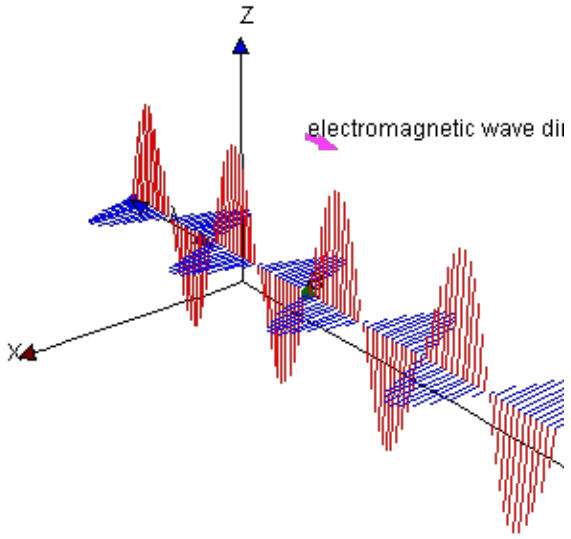
AIRBUS

Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

Base Télécom
Propagation des ondes radio

Behaviour of electromagnetical waves when they are transmitted, propagated from one point to another travelling through different medium and/or environments



= a world of adventures !

AIRBUS

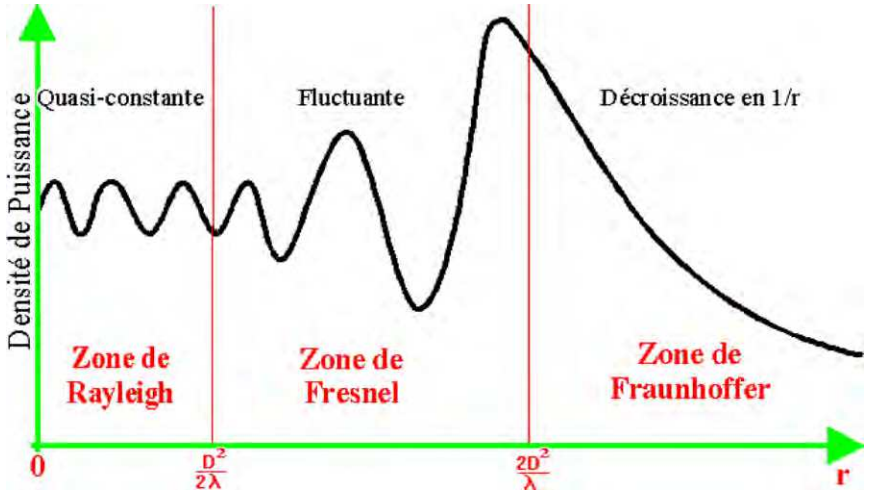
Base Télécom
Propagation des ondes radio

Free Space propagation:

- In free space, all electromagnetic waves (radio, light, X-rays, etc.) obey the inverse-square law which states that the power density of an electromagnetic wave is proportional to the inverse of the square of the distance from a point source or:
  Free Space Path Loss or FSPL

$$\mathrm{FSPL} = \left(\frac{4\pi d}{\lambda}\right)^2 = \left(\frac{4\pi df}{c}\right)^2$$

$$FSPL_{dB} = 20\log_{10}(f_{MHz}) + 20\log_{10}(d_{km}) + 32.44$$



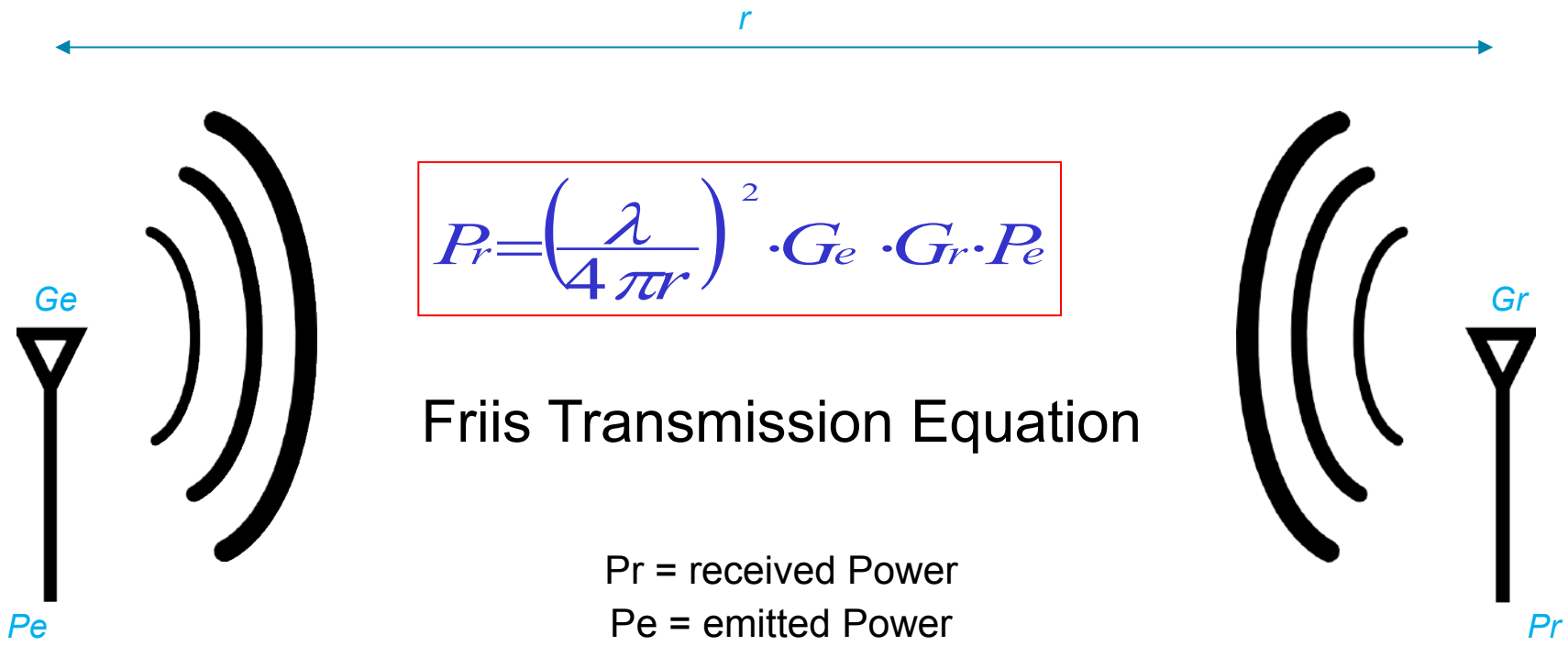
D= hauteur d'antenne

AIRBUS

Base Télécom

Propagation des ondes radio

- Transmission ←→ Réception



$$Pr = \left(\frac{\lambda}{4\pi r}\right)^2 \cdot Ge \cdot Gr \cdot Pe$$

Friis Transmission Equation

Pr = received Power
Pe = emitted Power
Ge = Antenna Gain – emitting side
Gr = Antenna Gain – receiving side
λ = wavelength (λ = 2π *f*)
r = distance

AIRBUS

Base Télécom
Propagation des ondes radio

- Transmission ←→ Réception – *version dB*
  - En expression logarithmique, donc en dB:

$$Pr=Pt+Gt+Gr+FSPL$$

  - Avec :
    - *Pr, Pt*: Puissance reçue/émise en dBm ou dBW
    - *Gr, Gt*: gain de l'antenne de réception/d'émission en dBi
    - *FSPL*: pertes de propagation en dB

$$\text{FSPL}=20\log(c/4\pi f d)$$

    - *c*: vitesse de la lumière en ms^{-1}
    - *f*: fréquence radioélectrique en Hz
    - *d*: distance en m
- En changeant les unités, on trouve

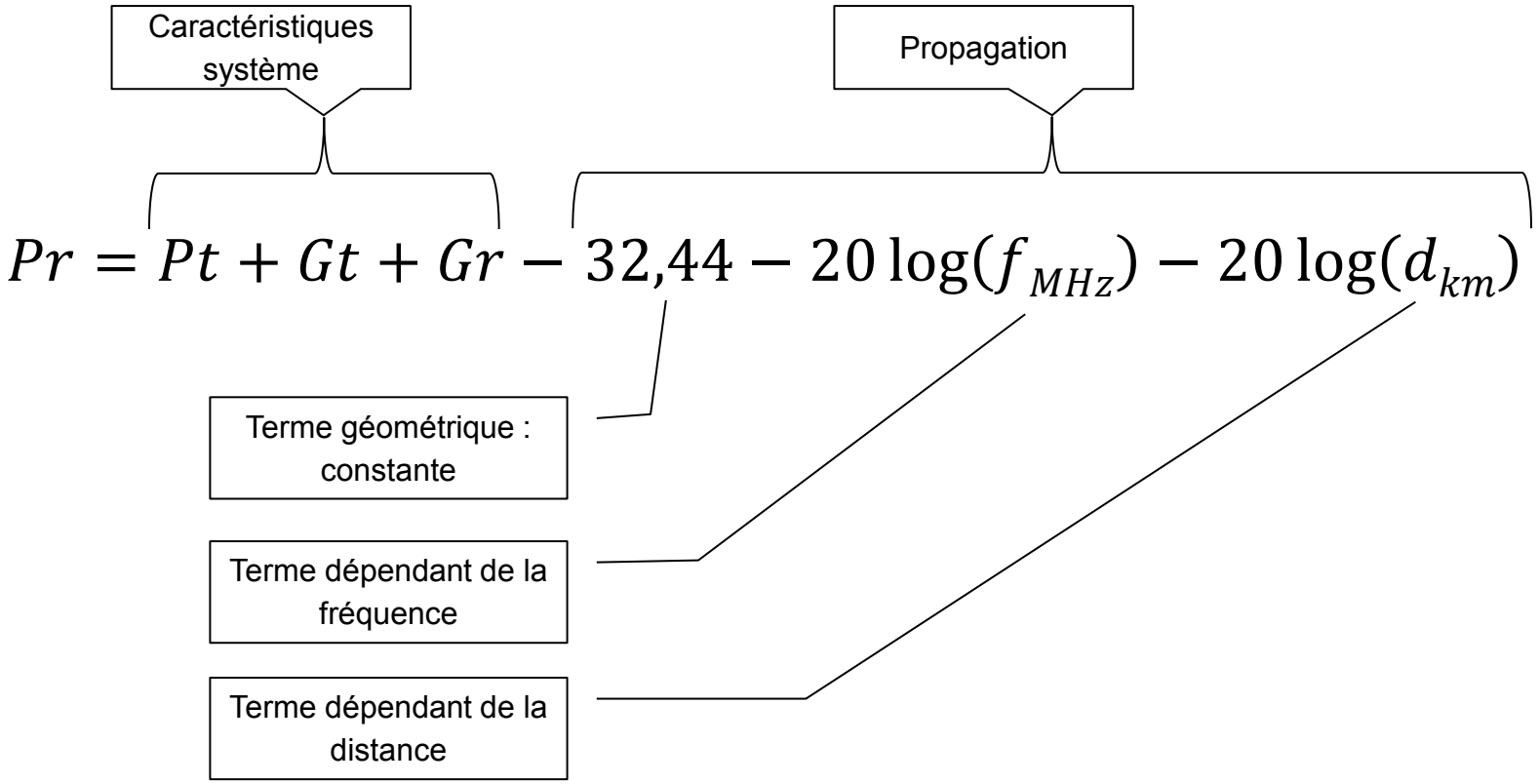
$$\text{FSPL} = -20\log\left(\frac{40\pi}{3}\right) - 20\log(f_{MHz}) - 20\log(d_{km})$$

$$FSPL = -32{,}44 - 20\log(f_{MHz}) - 20\log(d_{km})$$

Base Télécom

Propagation des ondes radio

- Transmission ←→ Réception – *version dB*



AIRBUS

Base Télécom
Propagation des ondes radio

- Transmission ←→ Réception – *version dB*

Passage vers le monde réel …

$$Pr = Pt + Gt + Gr - 32{,}44 - 20\log(f_{MHz}) - 20\log(d_{km}) - \mathrm{P1} - \mathrm{P2}$$

Avec :

- **P1**: Pertes de propagation supplémentaires (monde réel)
- **P2**: Pertes système (système réel)

P1 ne dépend pas de la conception système, mais des lois physiques de propagation dans un monde qui n'est pas idéal (absorption, diffraction, réflexions multiples, masquages, …). Ce terme est difficile à appréhender et à quantifier

P2 dépend de la conception système: type et longueurs de câbles, choix de la connectique, placement des antennes, désadaptations, …

Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses)

1. *Free Space Loss* $FSPL_{dB} = 20\log_{10}(f_{MHz}) + 20\log_{10}(d_{km}) + 32.44$
2. *Impedance (mis) matching: antenna efficiency*
3. *Noise: device (electronics) & environment (atmospherical noise, cosmical noise + interferences)*
4. *Obstacles*
5. *Multiple / Multipath Reflections*
6. *Diffraction*
7. *Climate: humidity, rain, dust particles, …*
8. *Environment: materials, vegetation, …*
9. *Doppler effect*

Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses) Impedance (mis) matching: antenna efficiency

- *Isotropic Radiator*

A_{er} is the effective area of the emitting/receiving antenna.

The effective area A_{er} is linked with the physical surface A_p :

$$A_{er}=\eta A_p$$

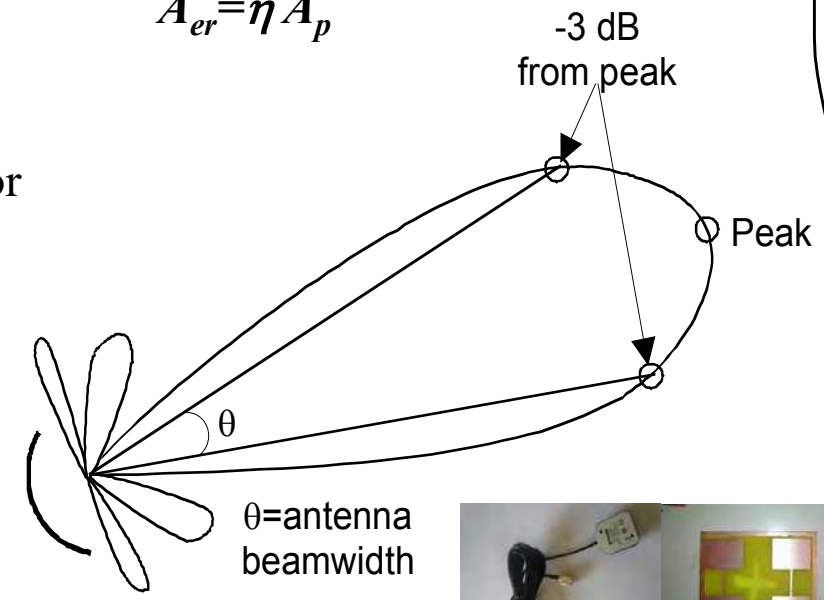
with η the antenna efficiency.

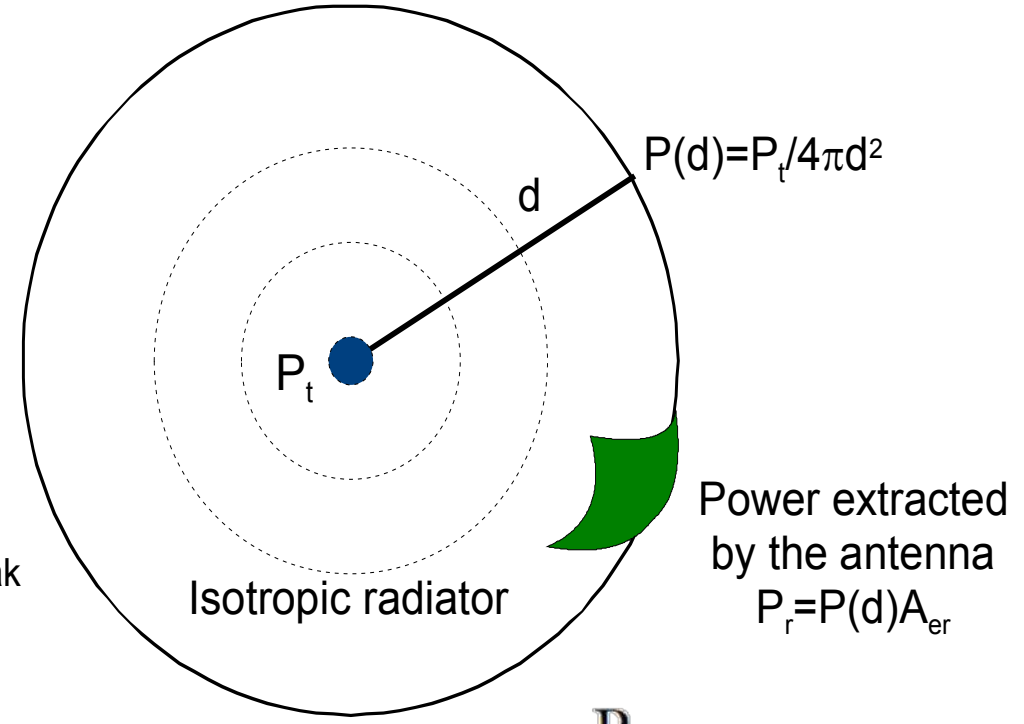
η = 0.55 for a parabolic reflector

η = 0.75 for a horn antenna

$$G=A_{er}/A_{ei}=4\pi A_e/\lambda^2$$

PIRE = Pt G





Power Density: $p(d)=\frac{P_t}{4\pi d^2}\ W/m^2$

AIRBUS

Base Télécom
Propagation des ondes radio

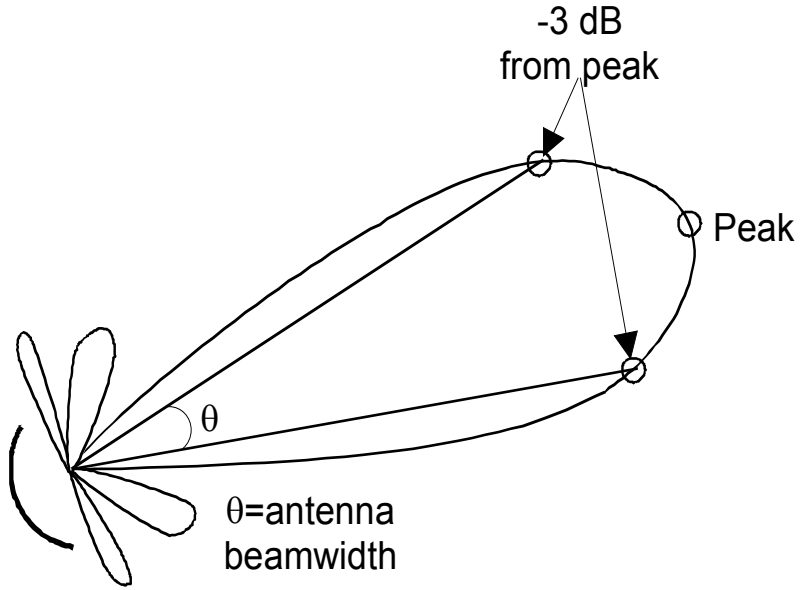
- Pertes (Impairments & Losses) Impedance (mis) matching: antenna efficiency

- *Pertes de pointage*

- *Pertes de polarisation*
  - la perte de polarisation est de la forme:

$$Ppolar = -20\log(\cos\theta)$$

  - θ étant l'angle entre les deux antennes
  - En pratique pour θ=20°, Ppolar= -0,5dB



Base Télécom
Propagation des ondes radio

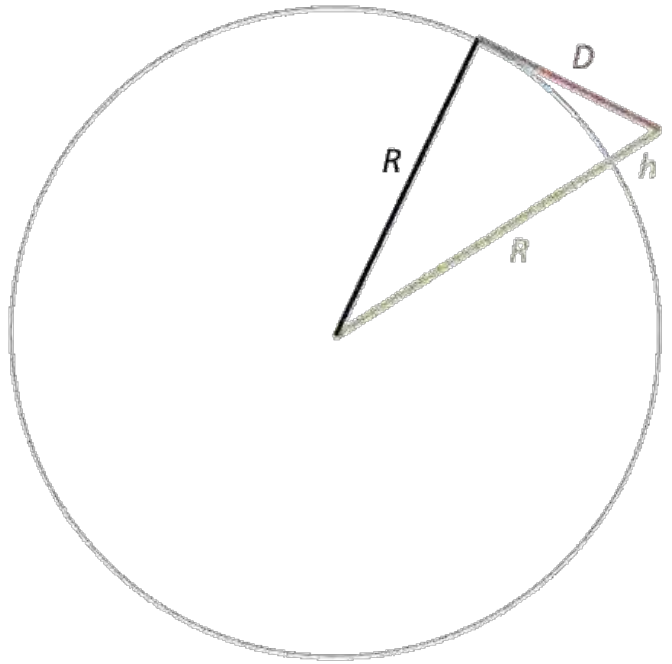
- Pertes (Impairments & Losses)

Noise: device (electronics) & environment (atmospherical noise, cosmical noise + interferences)
Obstacles

Condition de visibilité géométrique: $$dm = \sqrt{2Rt}\left(\sqrt{h1} + \sqrt{h2}\right)$$

- h1: hauteur de l'émetteur
- h2: hauteur du récepteur
- Rt: rayon terrestre
- Dm: distance maximale

- **C'est une condition nécessaire mais pas suffisante**



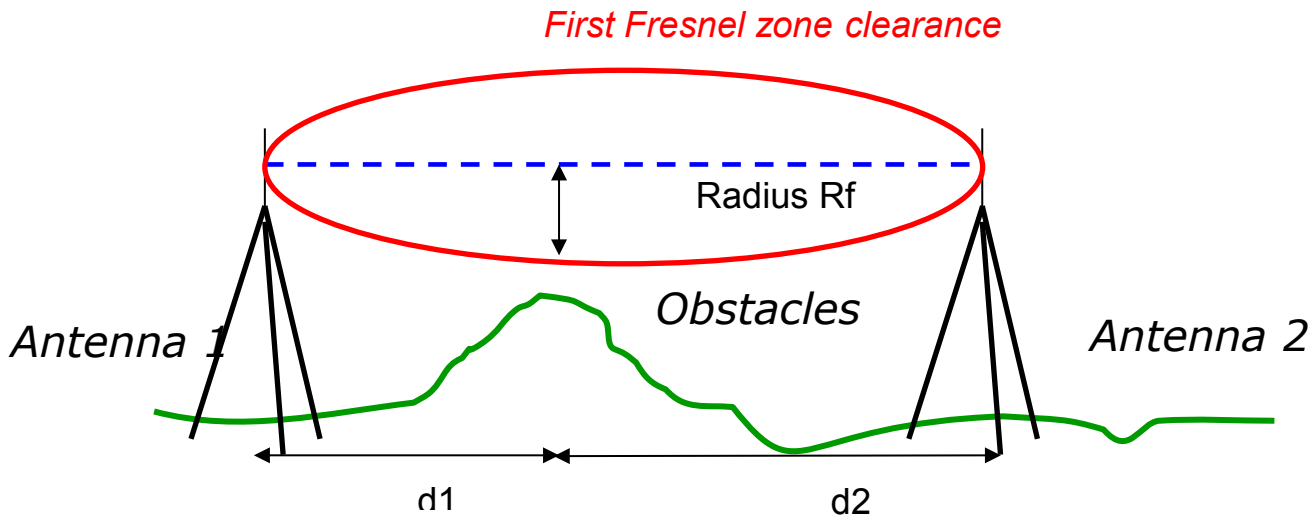
$$R^2 + D^2 = (R+h)^2 = R^2 + 2Rh + h^2$$
$$D = \sqrt{2Rh + h^2} \simeq \sqrt{2Rh}$$

Base Télécom
Propagation des ondes radio

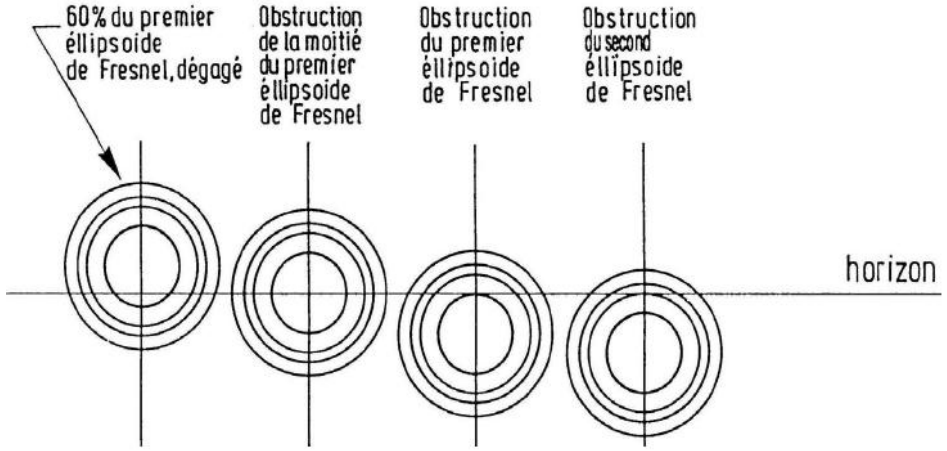
- Pertes (Impairments & Losses)

Obstacles

- Visibilité en ligne de vue (LOS) de 2 antennes
  si respect de la non-obstruction du 1er ellipsoïde de Fresnel



$$R_f = \sqrt{\frac{\lambda d_1 d_2}{d_1 + d_2}}$$



λ	F	d = 50 km	r
0.5 µm	600 THz	Visible light (green)	0.08 m
5 cm	6 GHz	Centimetric waves	25 m
5 m	60 MHz	Metric waves	250 m
500m	600 kHz	Hectometric waves	2500 m

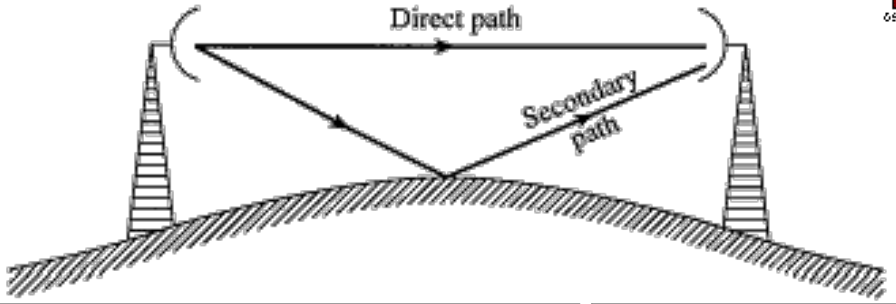
2 antennes @ 1km @ 2GHz
Obstacle à 500m
Rf vaut 6,124 mètres.

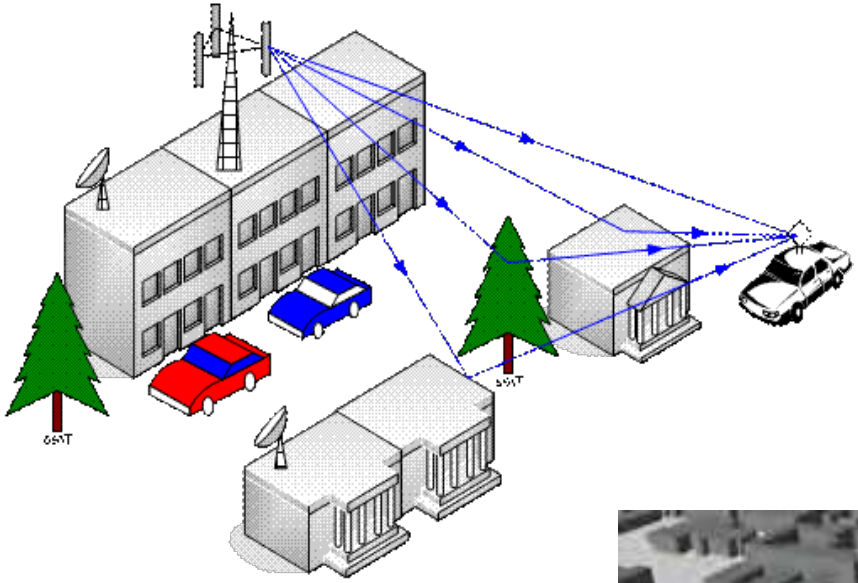
AIRBUS

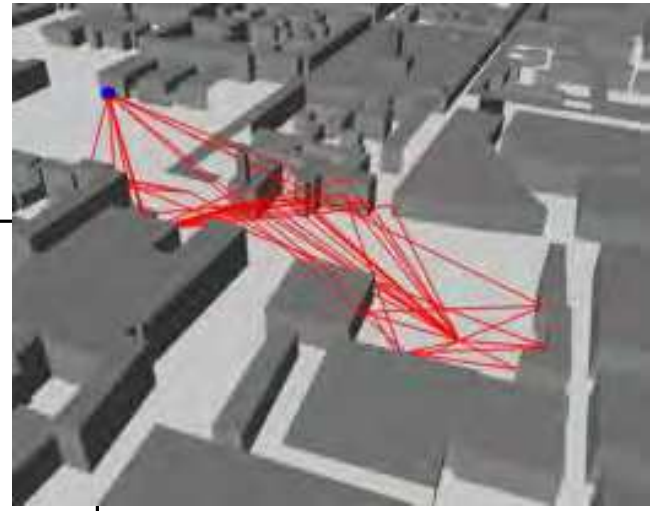
Base Télécom
Propagation des ondes radio

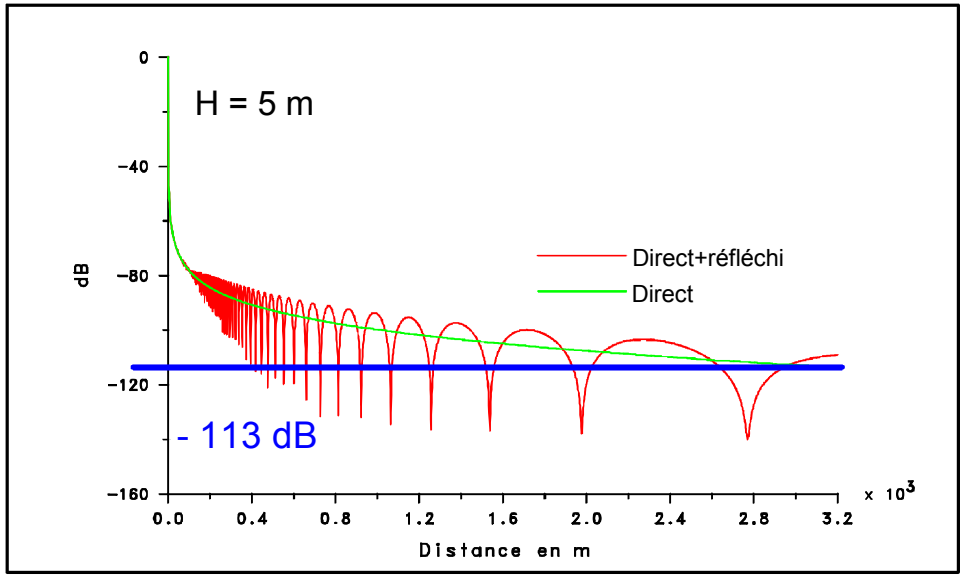
- Pertes (Impairments & Losses)

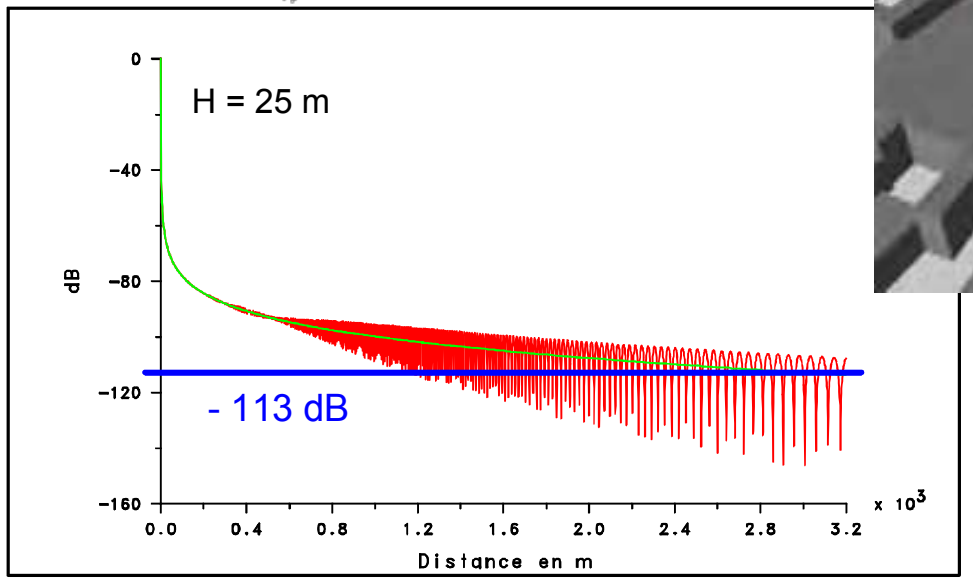
Multiple / Multipath Reflections











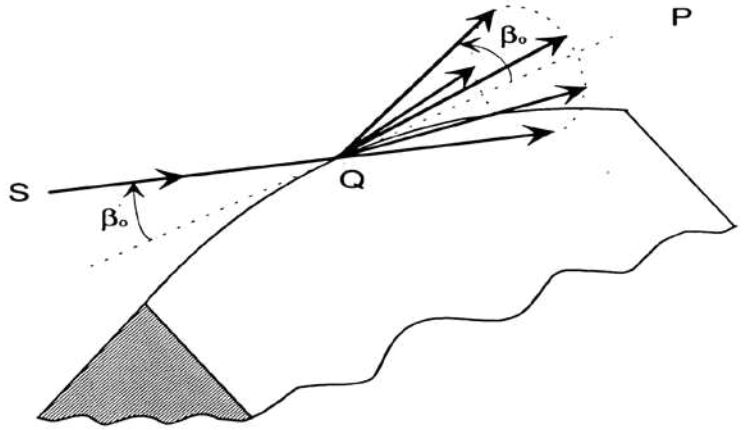
AIRBUS

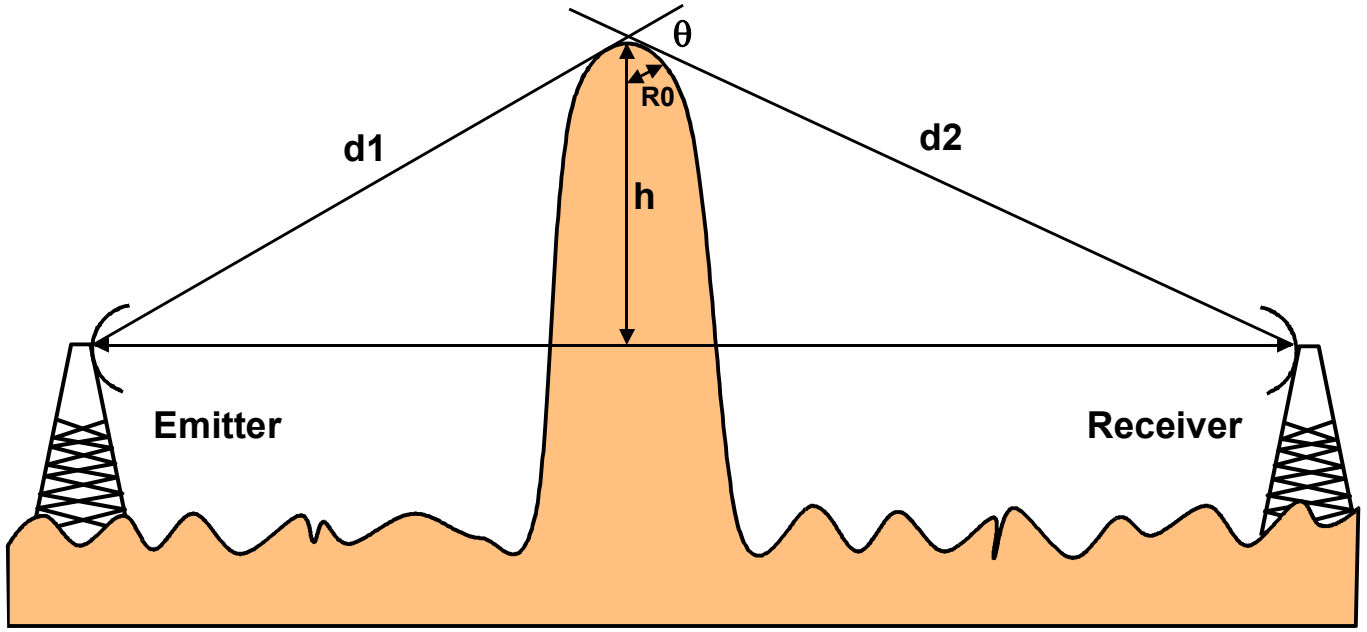
Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses)

Diffraction

La diffraction arrive lorsque le chemin de l'onde est partiellement ou totalement obstrué
Le principe de Huygens dit : chaque point touché par l'onde devient une source d'ondes sphériques





$$v = h \cdot \sqrt{\frac{2}{\lambda} \cdot \left(\frac{1}{d1} + \frac{1}{d2} \right)} = \theta \cdot \sqrt{\frac{2}{\lambda} \cdot \frac{d1 \cdot d2}{d}}$$

$$\rho = \sqrt{\frac{1}{d1} + \frac{1}{d2}} \cdot \left(\frac{\lambda \cdot R0^2}{\pi} \right)^{\frac{1}{6}}$$

AIRBUS

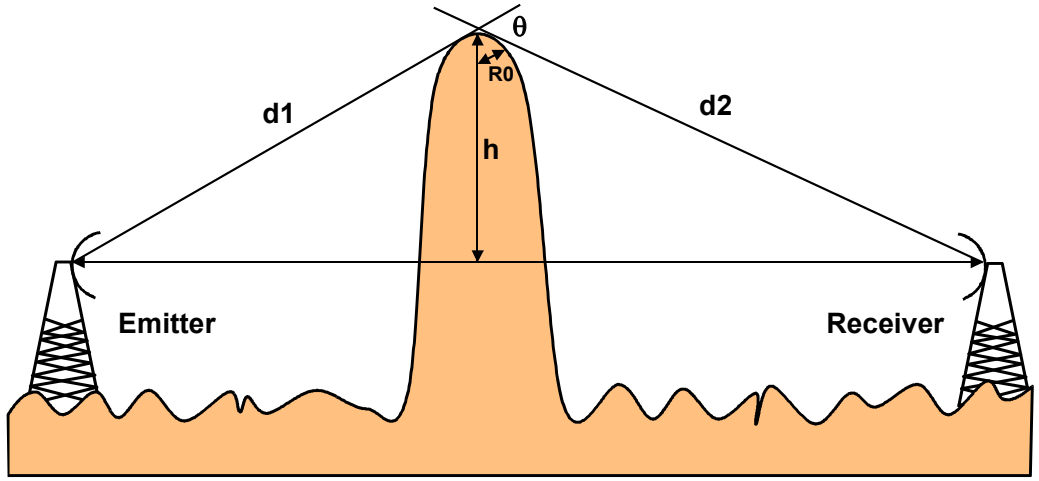
Base Télécom
Propagation des ondes radio

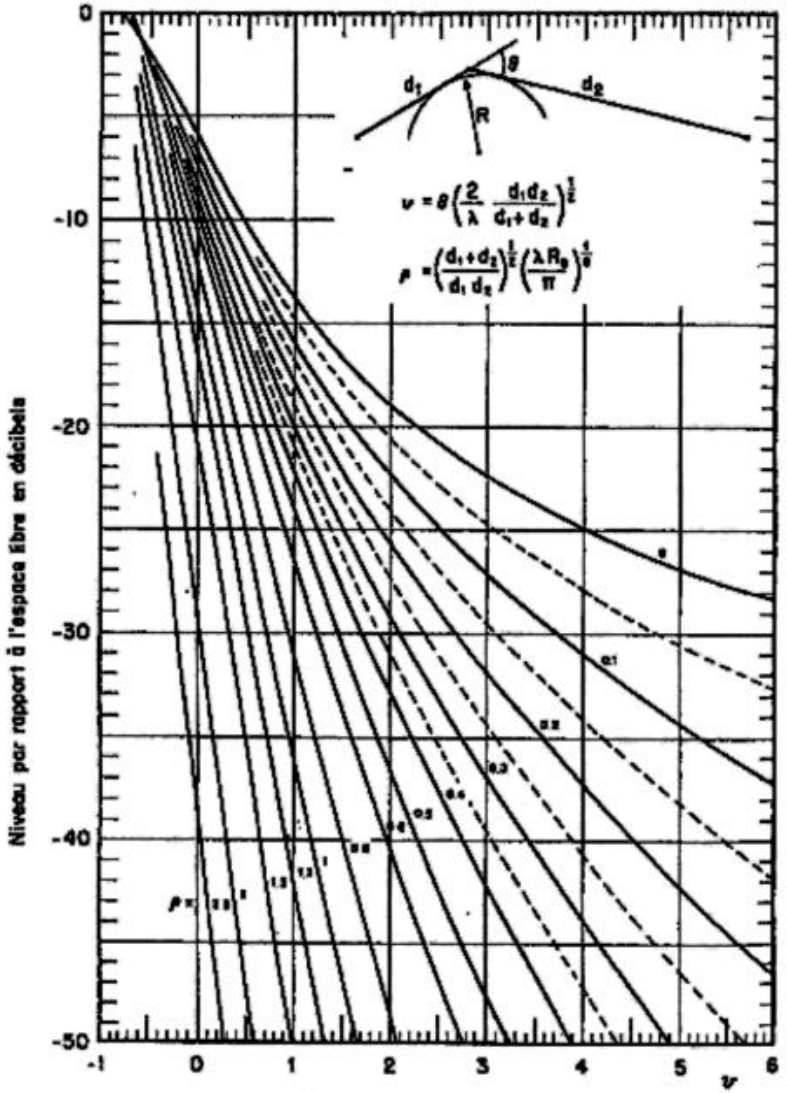
- Pertes (Impairments & Losses)

Diffraction

La diffraction arrive lorsque le chemin de l'onde est partiellement ou totalement obstrué
Lorsque R0 est proche de 0: (effet pointe)

$$A_{dB} = 6.9 - 20\log\left(\sqrt{(v-0.1)^2+1} - v + 0.1\right)$$





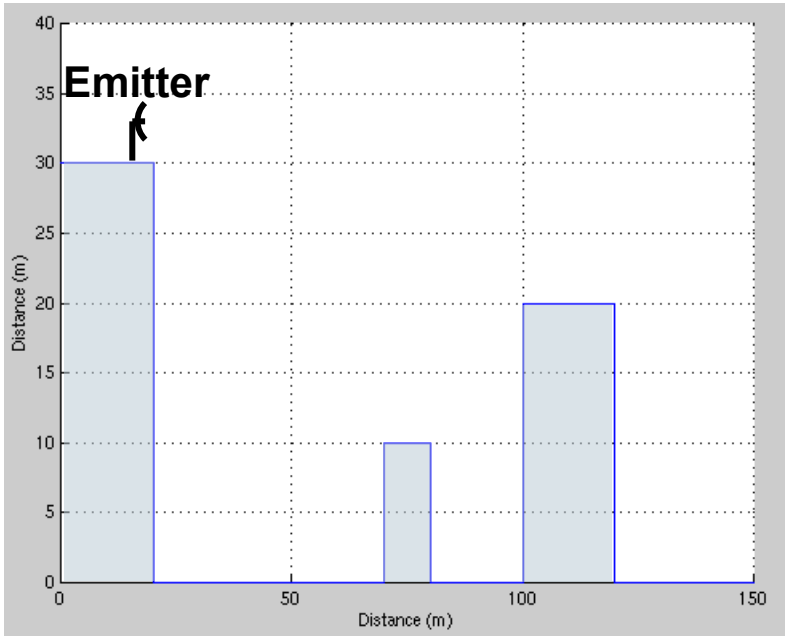
AIRBUS

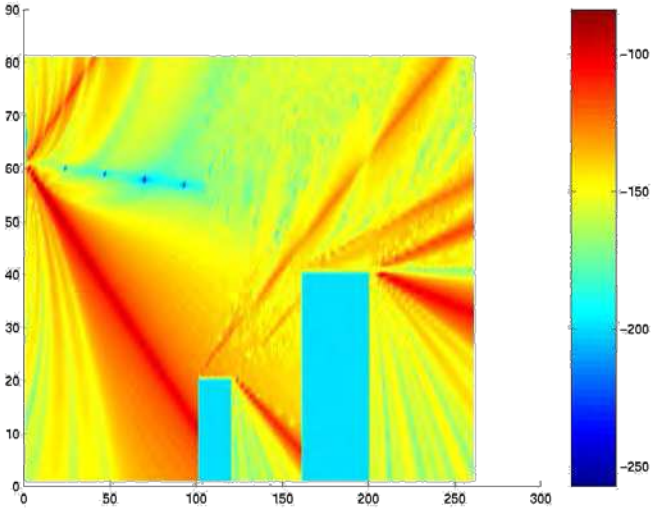
Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses)

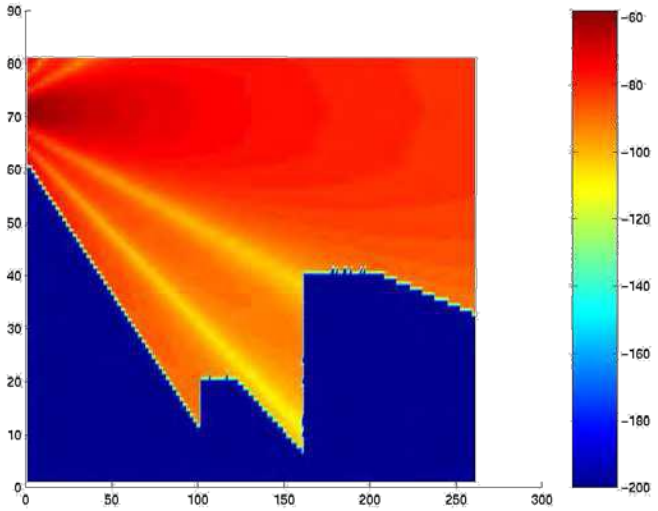
Diffraction

La diffraction arrive lorsque le chemin de l'onde est partiellement ou totalement obstrué
Lorsque R0 est proche de 0: (effet pointe)

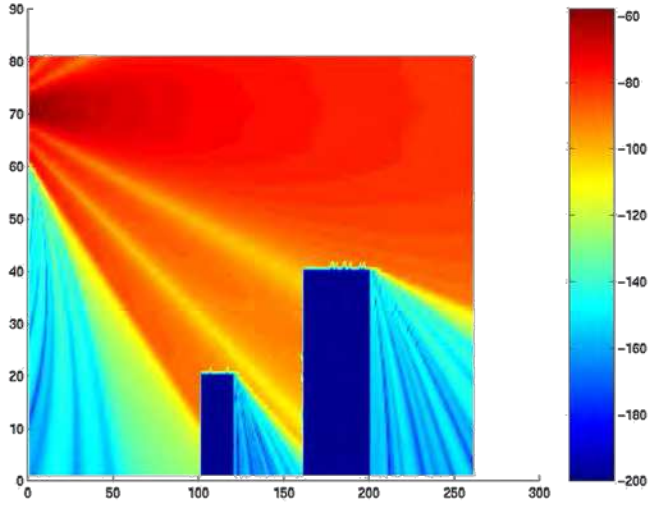




Diffracted waves only



Direct waves only



All waves

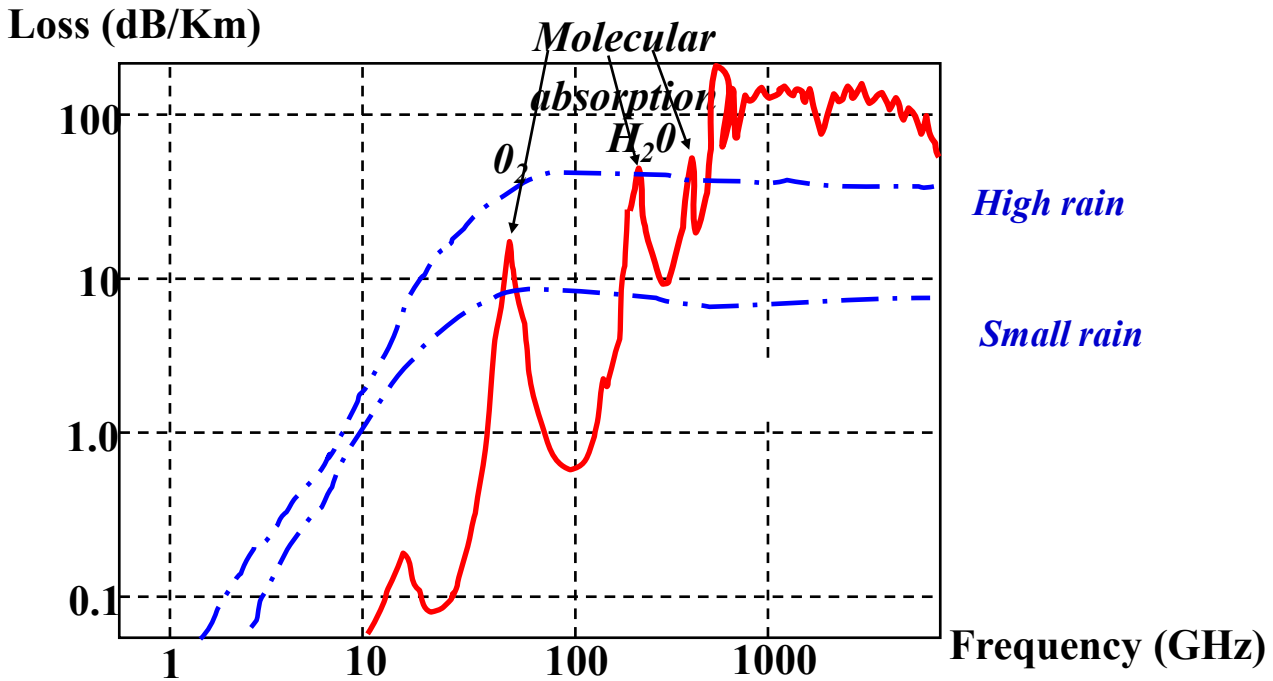
AIRBUS

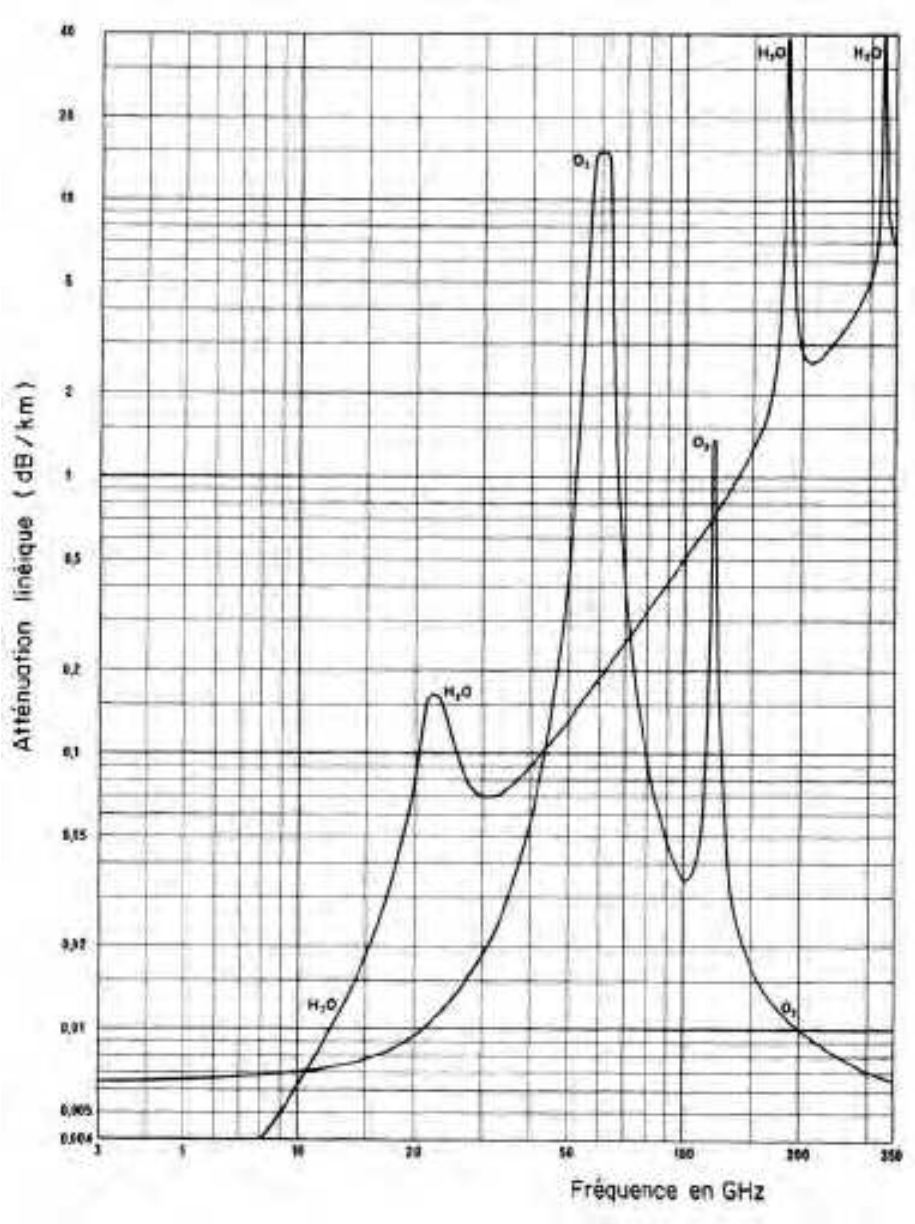
Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses)

Climate: humidity, rain, dust particles, …

- L'absorption dépend du matériaux
- L'absorption dépend de la fréquence





AIRBUS

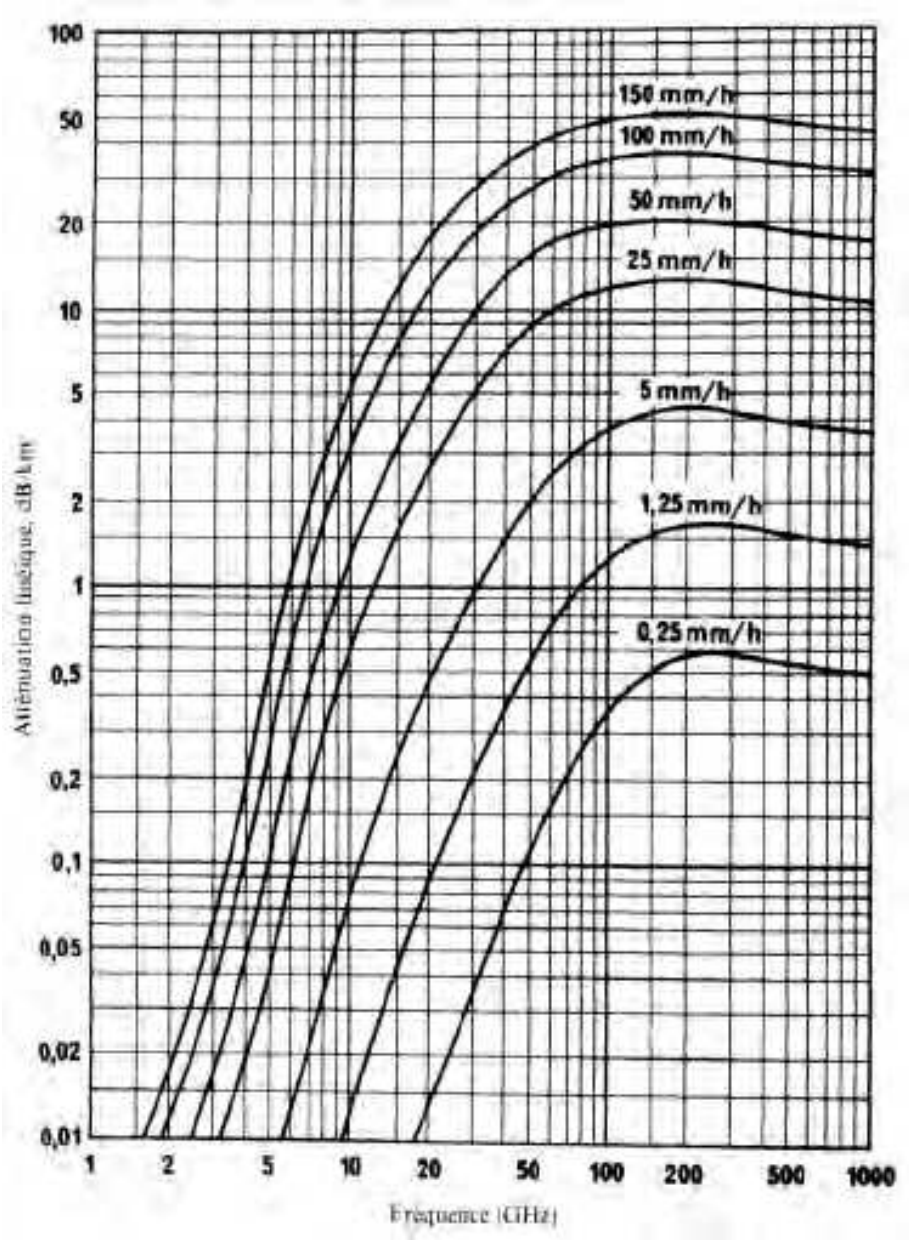
Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses)

Climate: humidity, rain, dust particles, …

- L'absorption dépend du matériaux
- L'absorption dépend de la fréquence

- Pluie



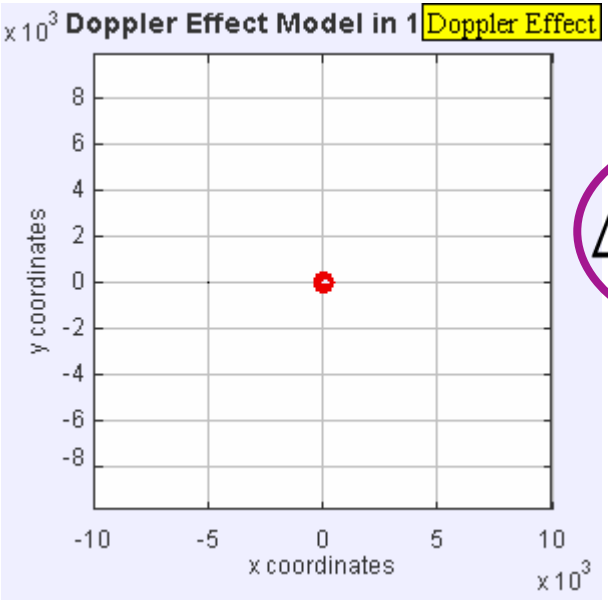
AIRBUS

Base Télécom
Propagation des ondes radio

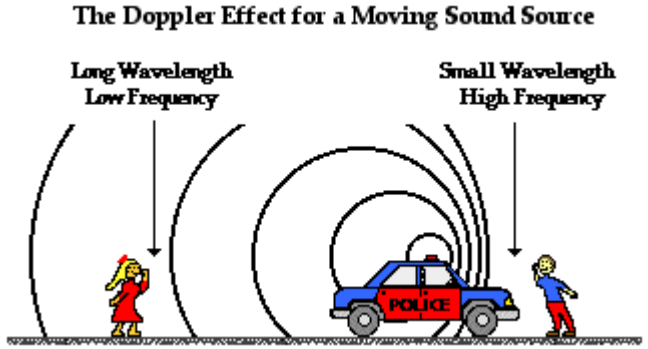
- Pertes (Impairments & Losses)

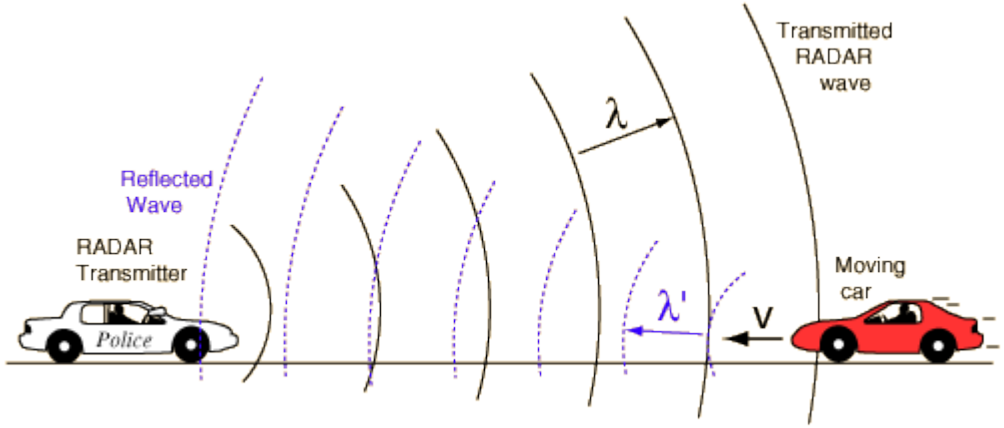
Doppler effect

Effet Doppler = décalage en fréquence du à la différence de vitesse



$$\Delta f = \frac{\Delta v}{c} f_0$$

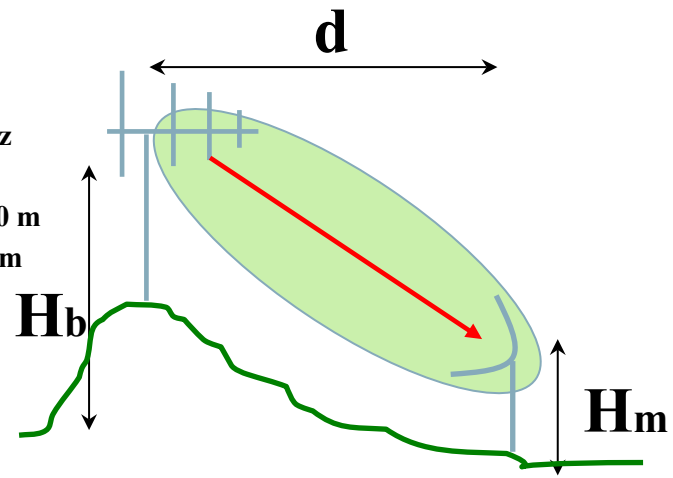


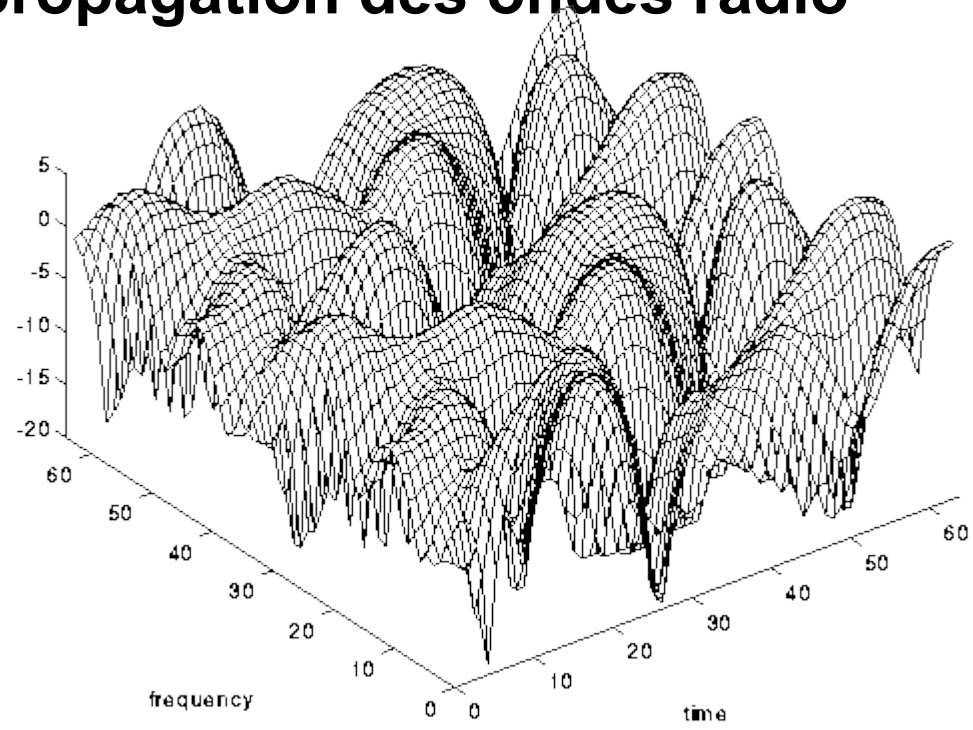


AIRBUS

Base Télécom
Propagation des ondes radio

- Pertes (Impairments & Losses)
- **La combinaison de tous ces effets rend la propagation des ondes radio hautement complexes et peu prédictible**





- **Input parameters :**
  - **f : frequency (MHz) between 100 & 1500 MHz**
  - **d : distance in km entre, from 1 to 20 km**
  - **Hb : height in m of the emitter, from 30 to 300 m**
  - **Hm : height in m of the receiver, from 1 to 20m**

Okumura-Hata Model – COST231 - Hata

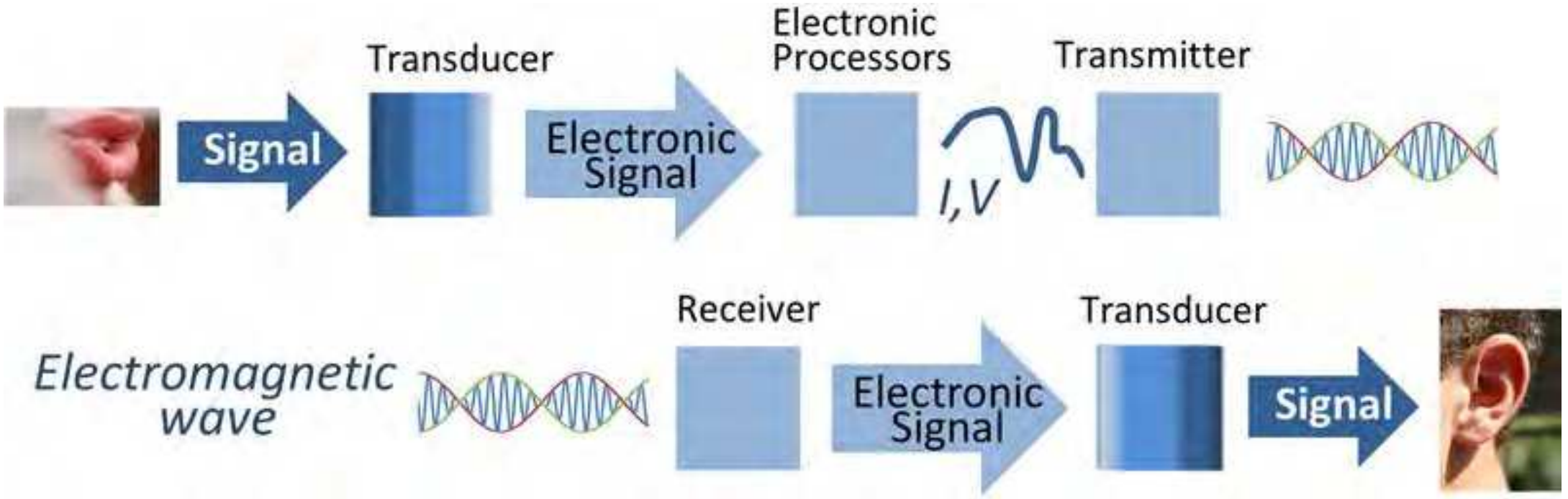
$$L_u(dB) = 69.55 + 26.16\log(f) - 13.82\log(H_b) - A(H_m) + (44.9 - 6.55\log(H_b)) \times \log(d)$$

AIRBUS

Base Télécom

Chaîne de transmission

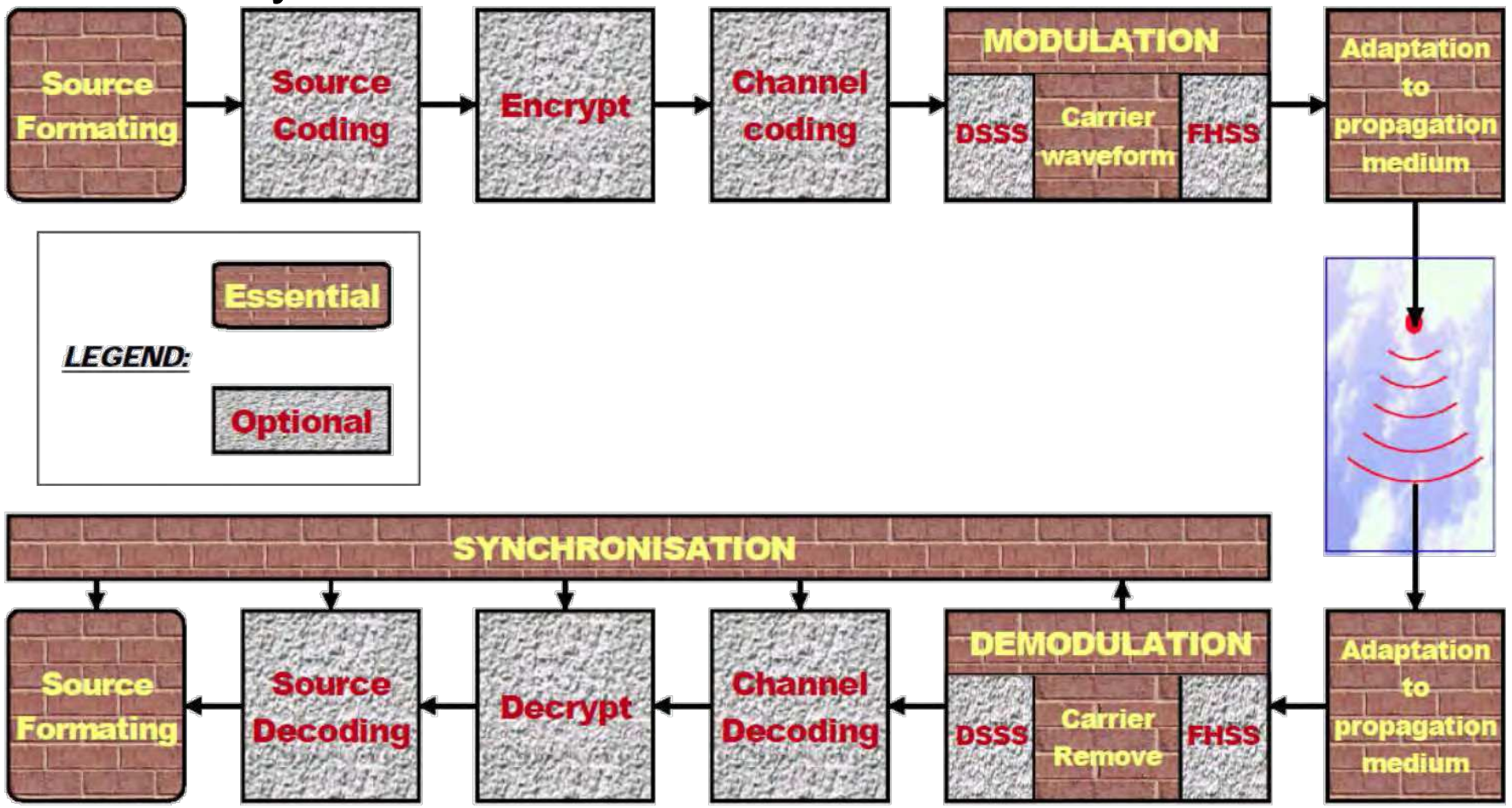
- Schéma d'un système de télécommunication sans fil pour la voix



AIRBUS

Base Télécom
Chaîne de transmission

- Composants d'un système de télécommunication sans fil



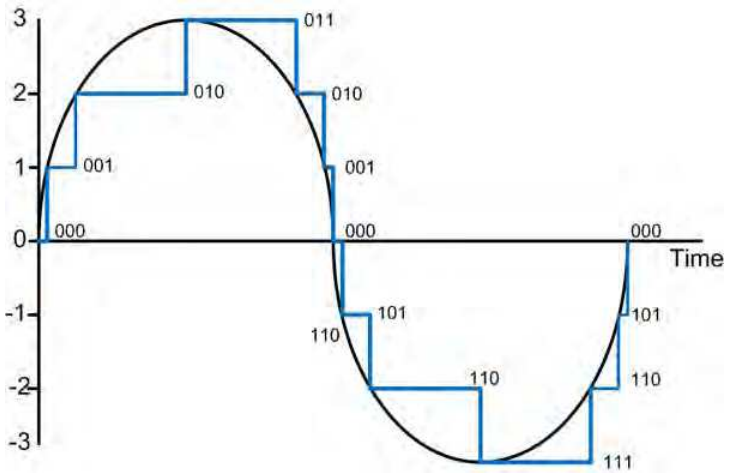
AIRBUS

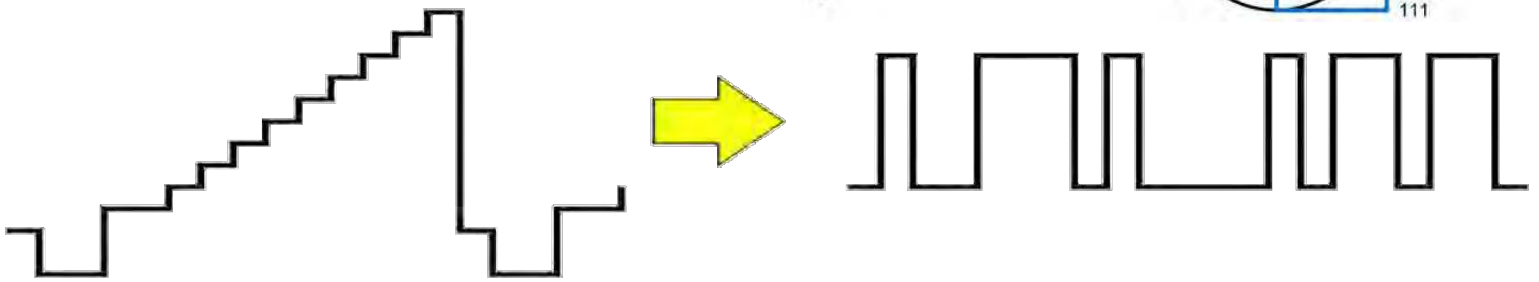
Base Télécom
Chaîne de transmission

- Source formating:

- Converts the signals from the source into signals that can be transmitted (typically bits)

Ex: Analog-to-Digital conversion of a video signal





AIRBUS

Base Télécom
Chaîne de transmission

- Source Coding & Decoding:

- Goal: to reduce the data rate of the source !

- Removal of redundancies (Lossless compressions)

  Ex: Winzip / 7Zip / WinRar / TIFF / FLAC lossless compressions

- Entropy reduction by the removal of non-necessary information (lossy compressions)

  Ex: MP3 lossy compression using psycho-acoustic criterions
  Jpeg /Divx / H264 & h265 (HEVC) lossy compression using psycho-visual criterions

Base Télécom
Chaîne de transmission

- Cyphering / Encryption / Scrambling:

- Turns the information scrambled or « non-readable » for un-authorized users / devices

Ex: AES 256 bits / SSL like

AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Adds redundancies to the signal to make it more robust to interferences (noise, …). Thus 2 advantages:
- Less power needed for transmission as the signal is more robust
- Adds integrity to received information

Ex 1: Hamming code transforms a byte into a 12 bit word
→ 1 error can be completely corrected

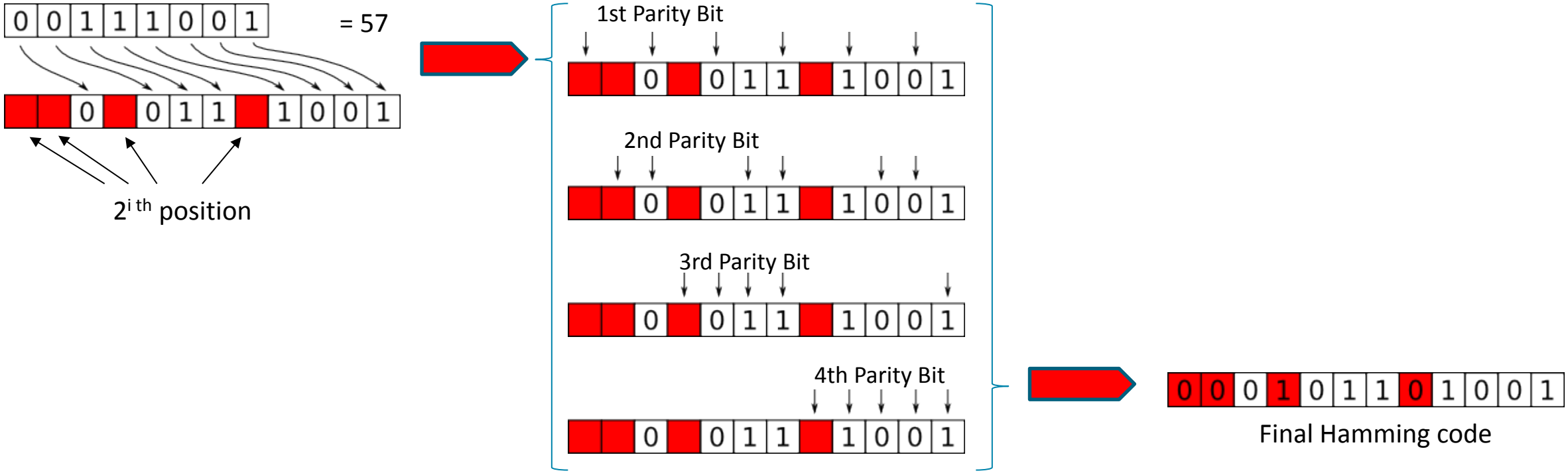
Ex 2: Convolutional Code with rate ½ and length 7 adds a bit to each input bit as a function of the previous 7 ones.

Ex 3: Turbo-codes

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 1: Hamming code transforms a byte into a 12 bit word (Block Code)



AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 1: Hamming code transforms a byte into a 12 bit word (Block Code)

Code efficiency = 8/12 = 2/3

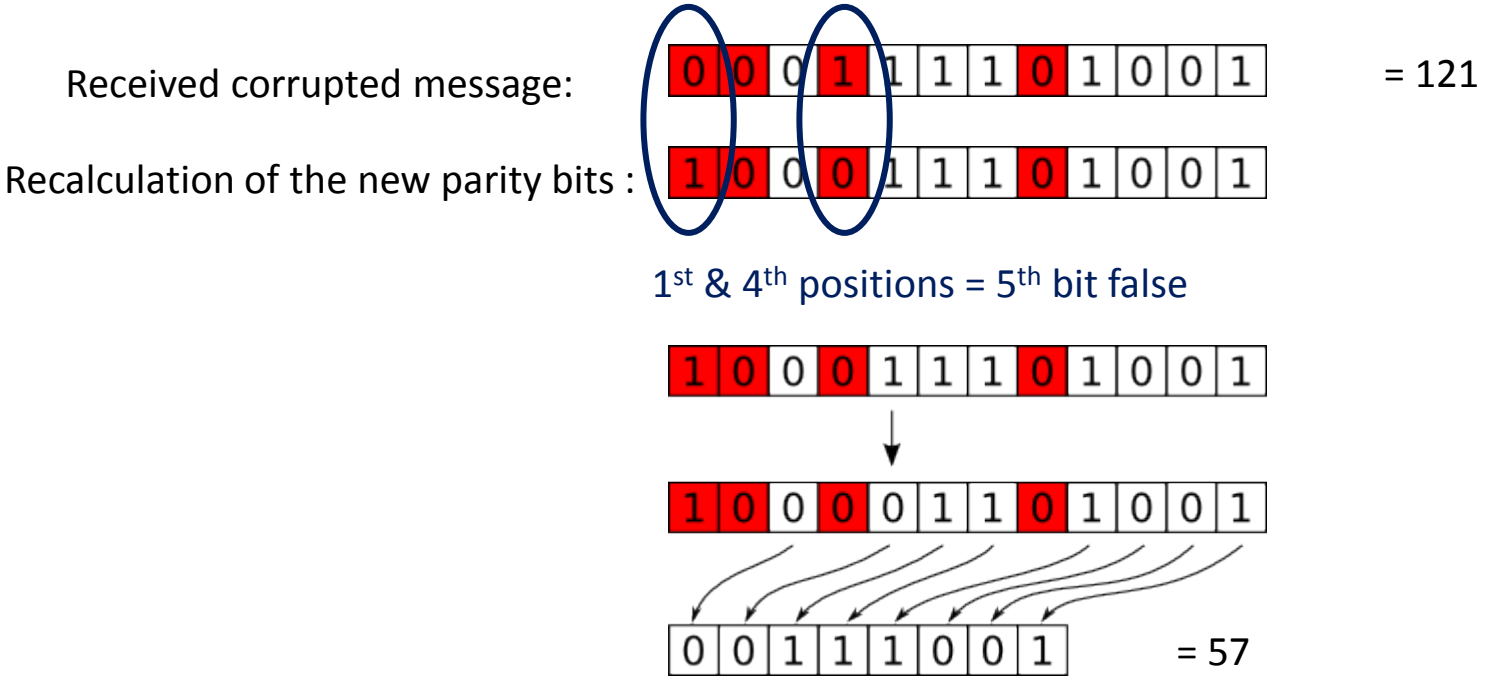
Without coding a Corrupted byte is received !
(=121)

0	1	1	1	1	0	0	1

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 1: Hamming code transforms a byte into a 12 bit word (Block Code)

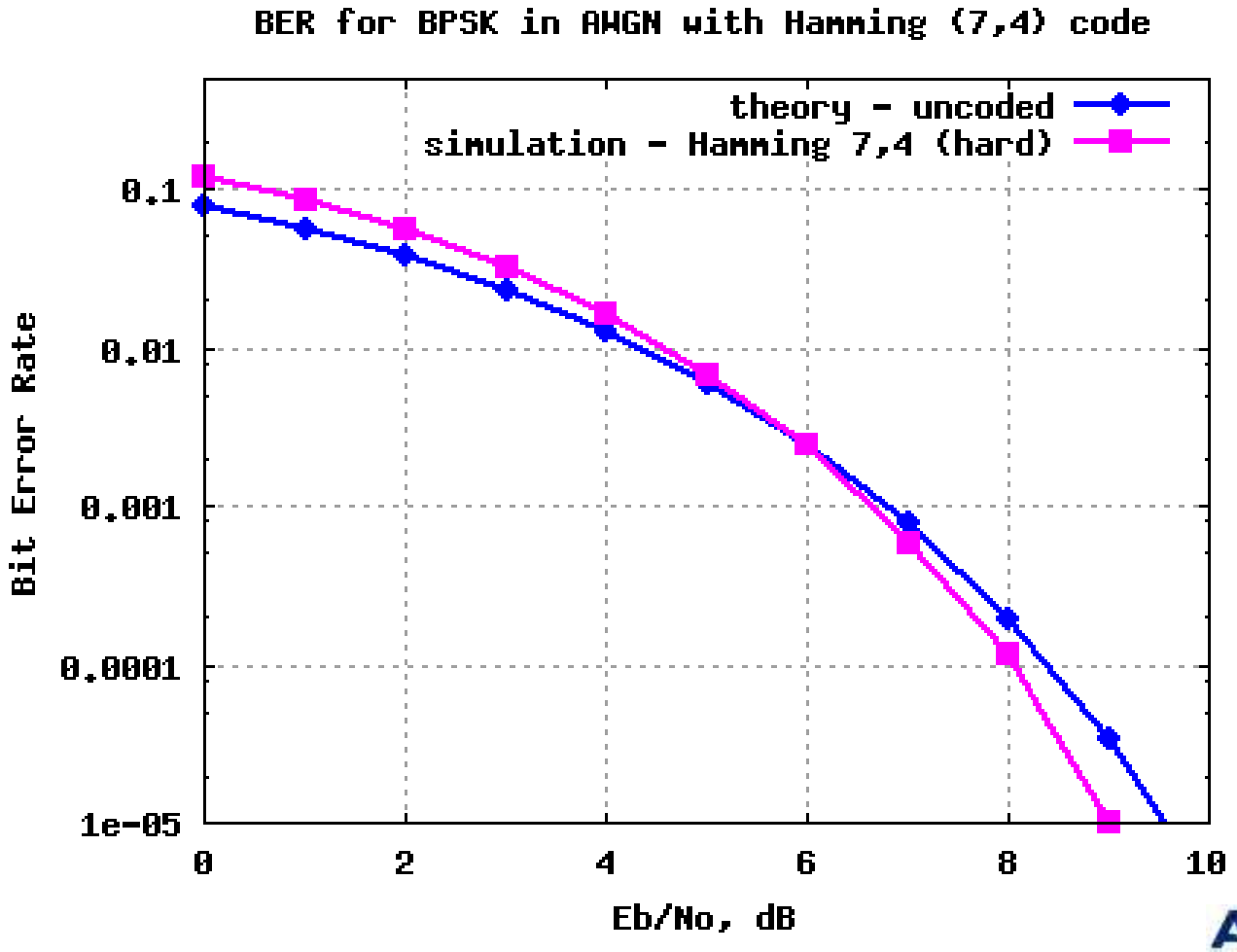


AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 1: Hamming code transforms a byte into a 12 bit word (Block Code)

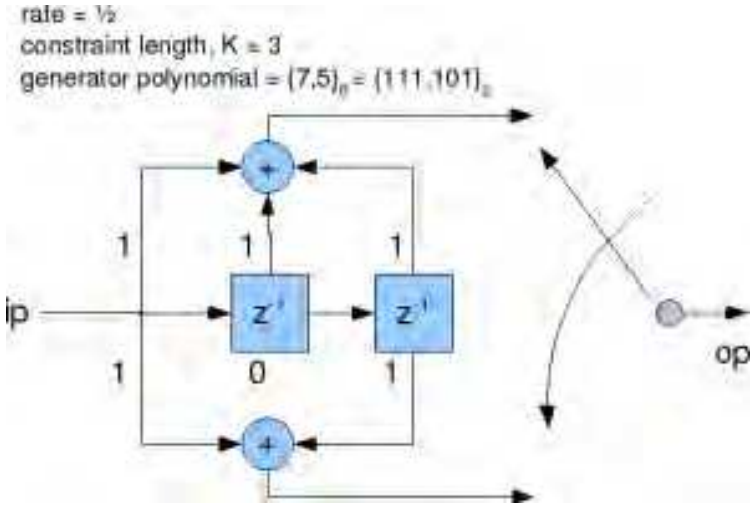


AIRBUS

Base Télécom
Chaîne de transmission

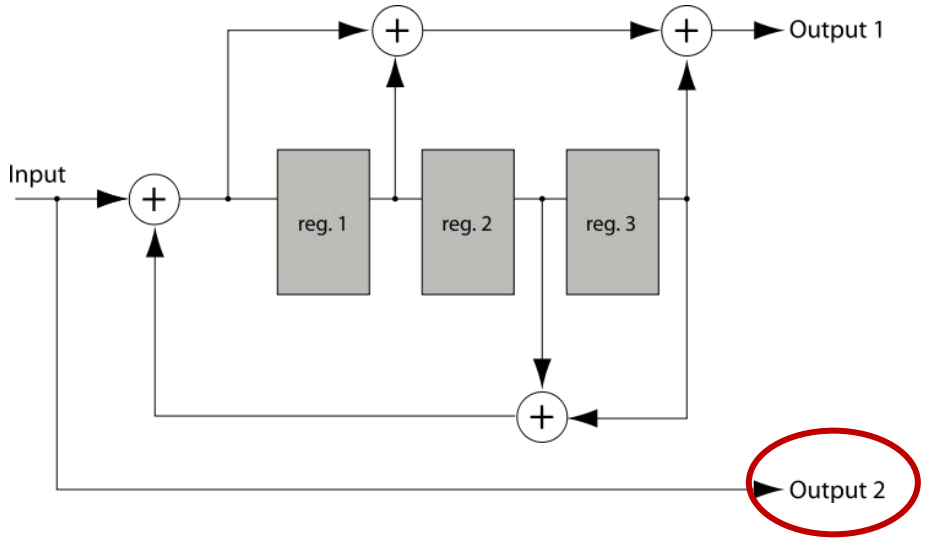
- Channel Coding:

- Ex 2: Convolutional Code with rate ½



Non recursive

= non systematic



Recursive

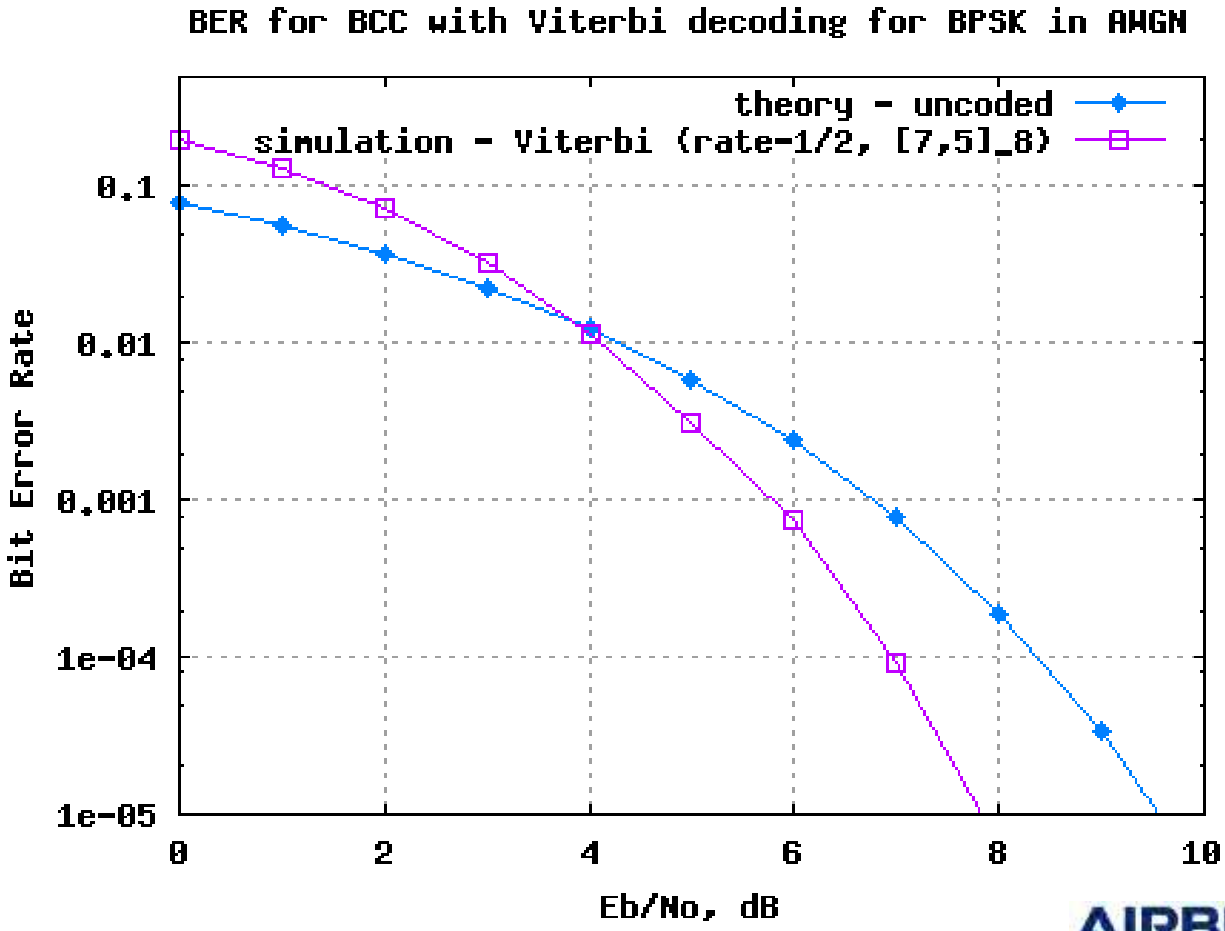
= systematic

AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 2: Convolutional Code with rate ½

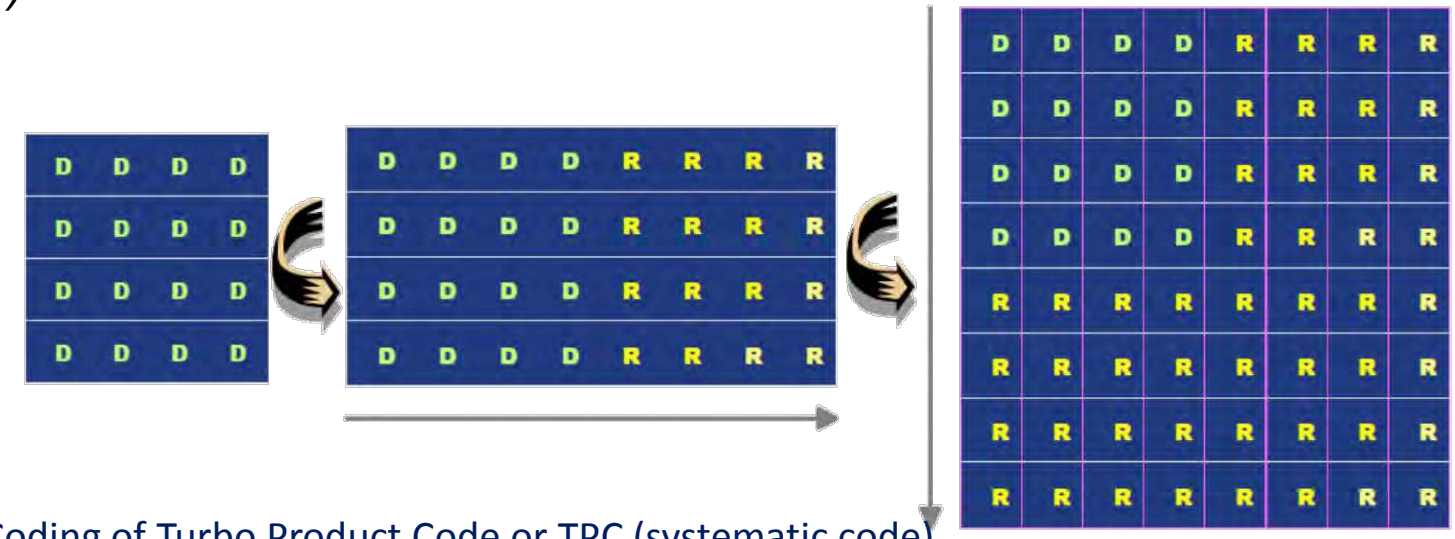


AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 3: Turbo-code
  (french innovation & Patent – 1993- by Berrou & Glavieux "Near Shannon Limit Error-correcting Coding and Decoding: Turbo-codes")



Coding of Turbo Product Code or TPC (systematic code)

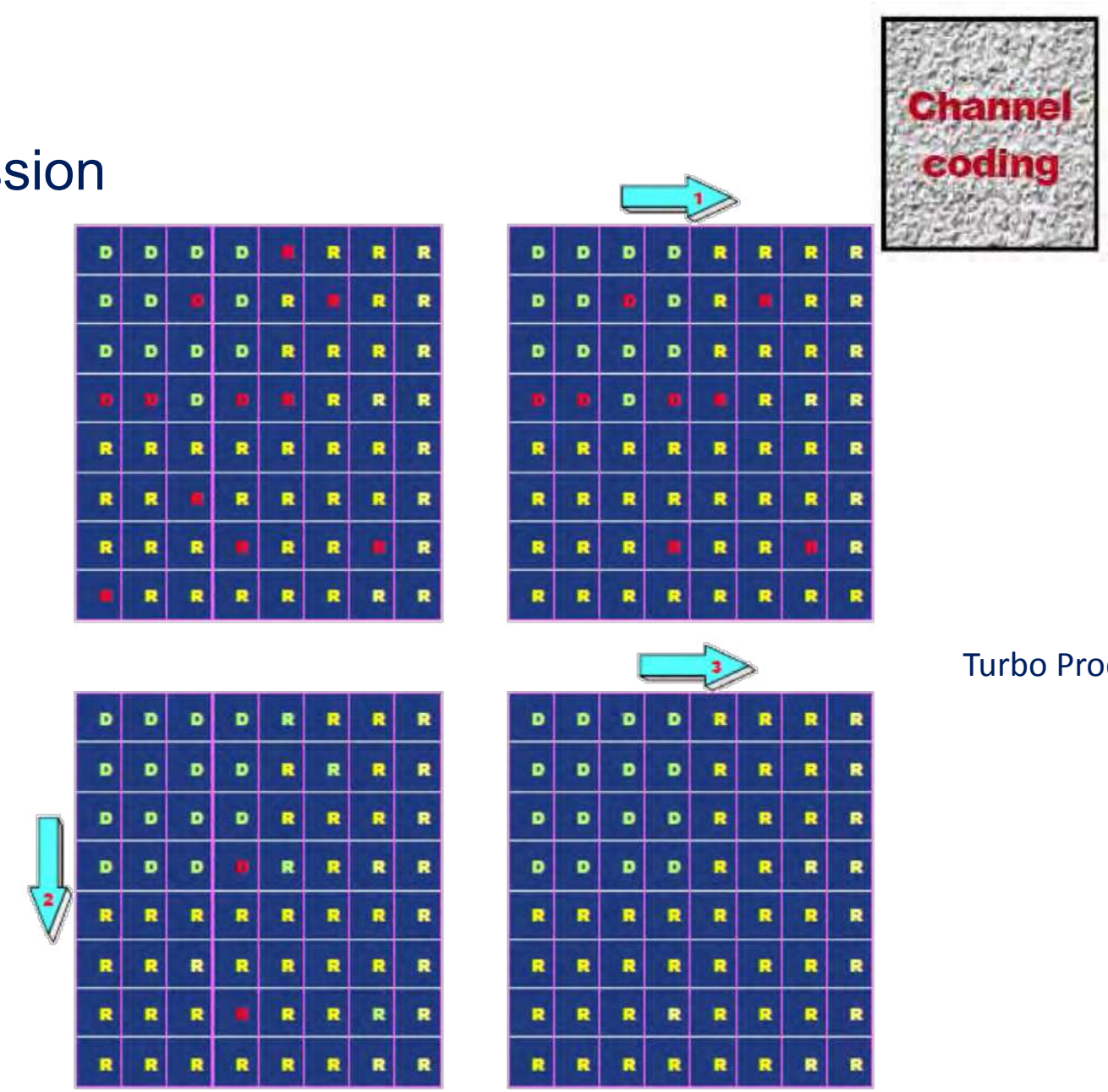
TPC $(8,4)^2$ with a coding rate of $(4/8)^2=1/4$

AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 3: Turbo-code



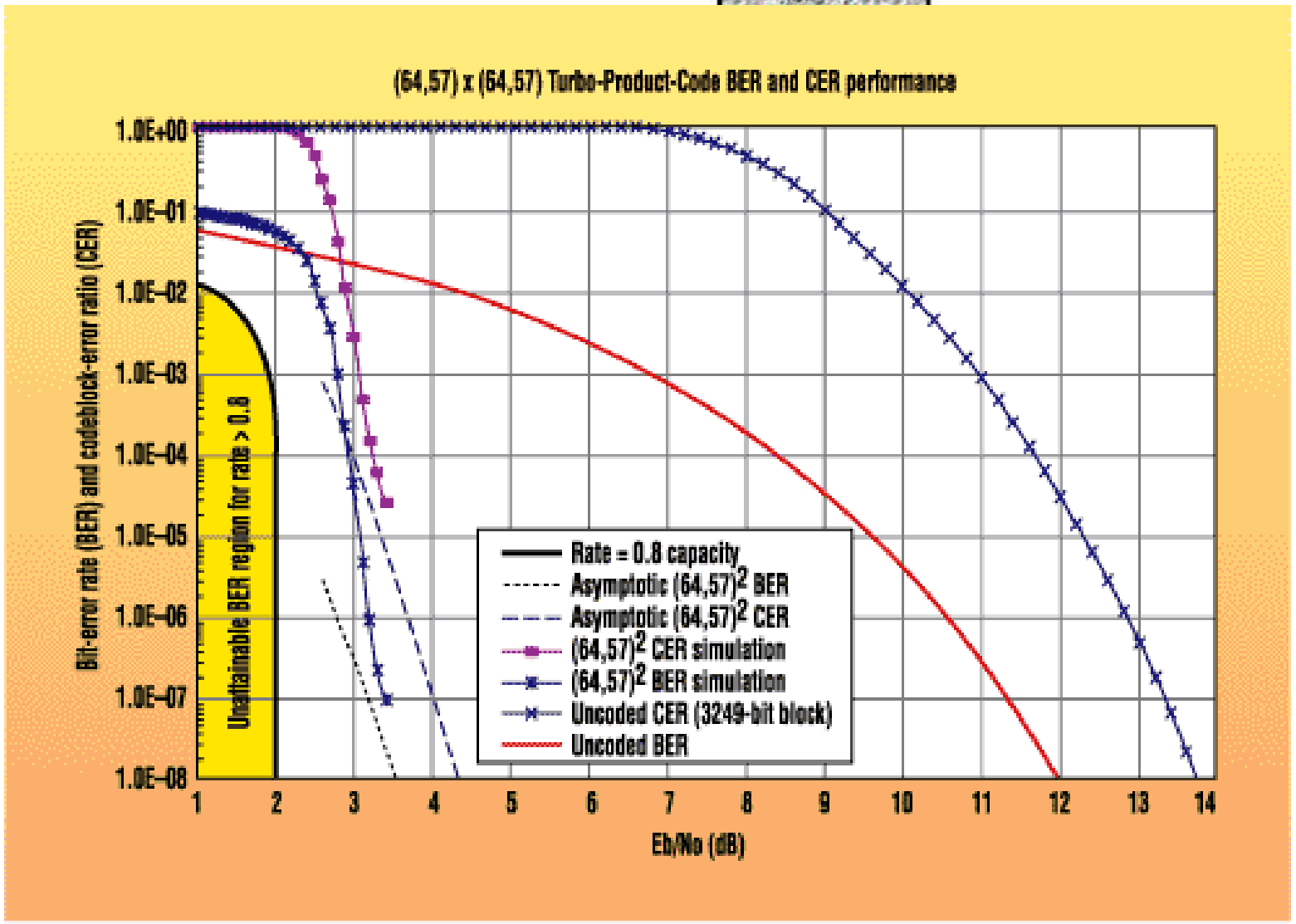
Decoding of
Turbo Product Code (systematic)

AIRBUS

Base Télécom
Chaîne de transmission

- Channel Coding:

- Ex 3: Turbo-code

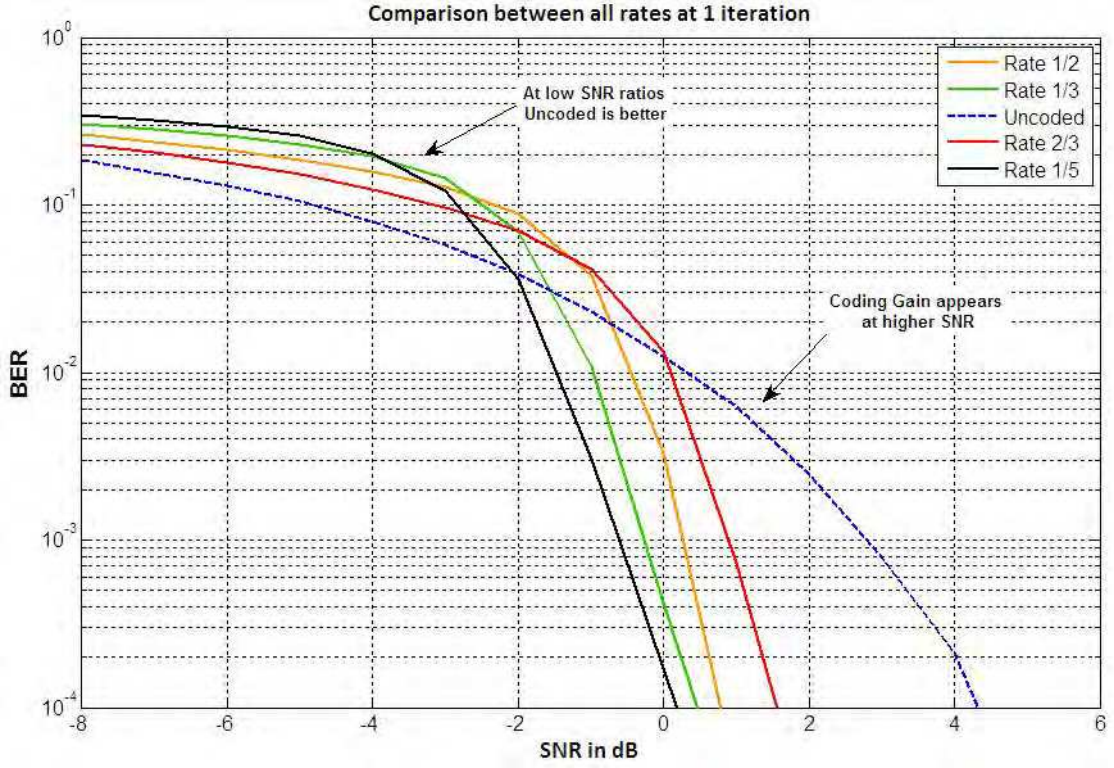


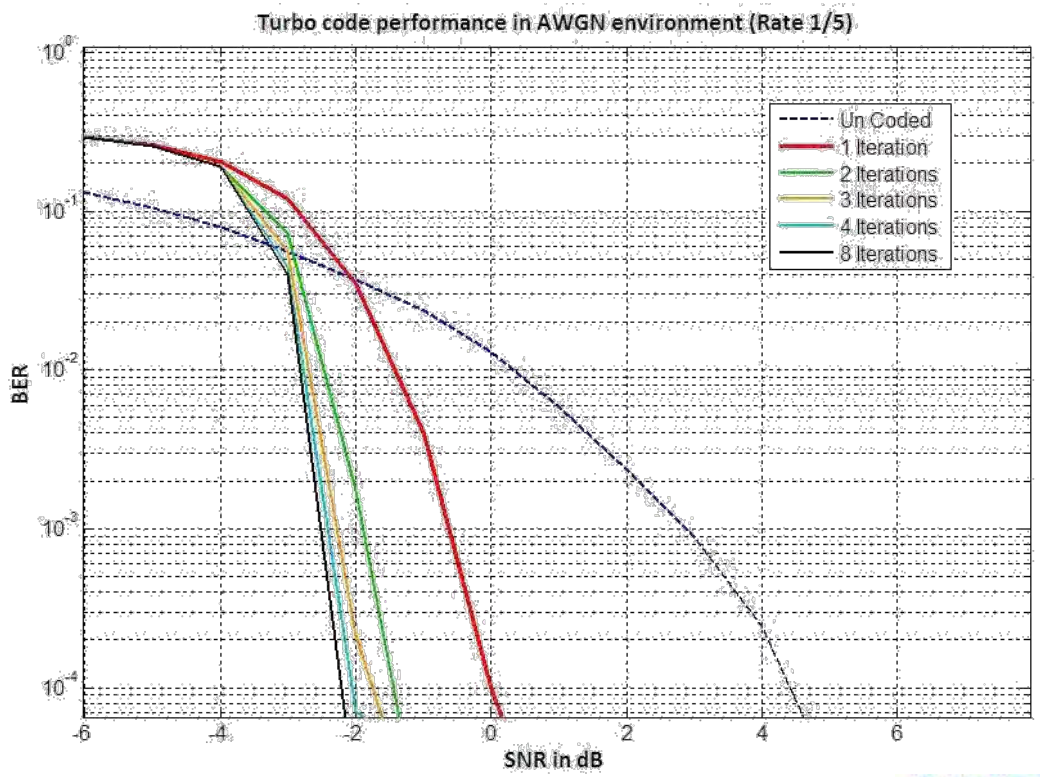
4. This graph shows the performance of a Turbo Product Code built from the (64,57) code used in both the x and y dimensions. Also included is a bit-error-rate plot of data transmitted without coding on the AWGN channel.

Base Télécom
Chaîne de transmission

- Channel Coding:

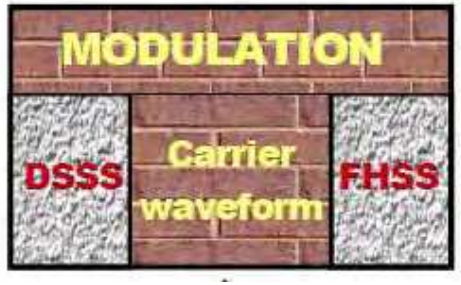
- Ex 3: Turbo-code





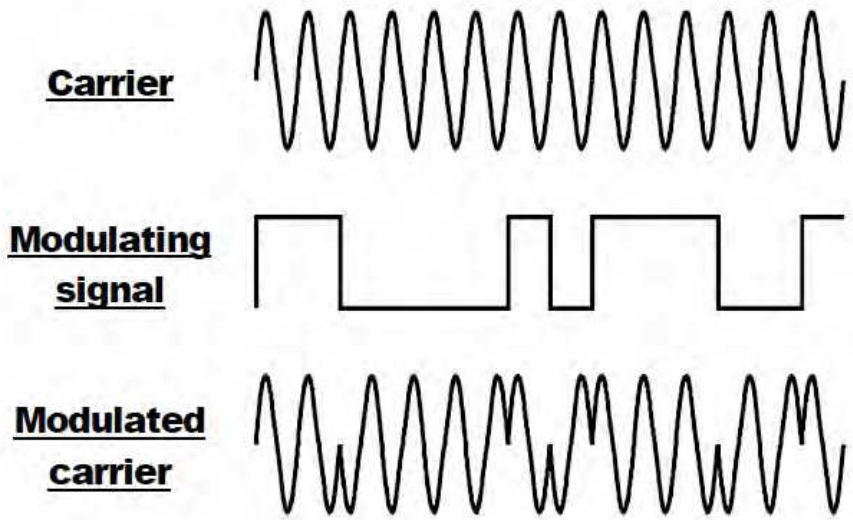
AIRBUS

Base Télécom
Chaîne de transmission



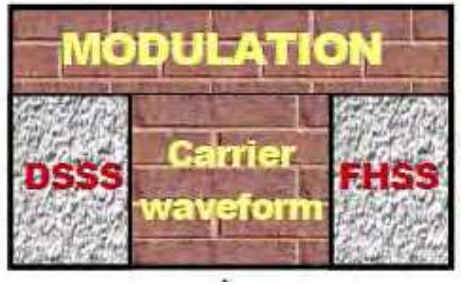
- Modulation:

- Converts the coded signal into an electrical waveform on a frequency carrier



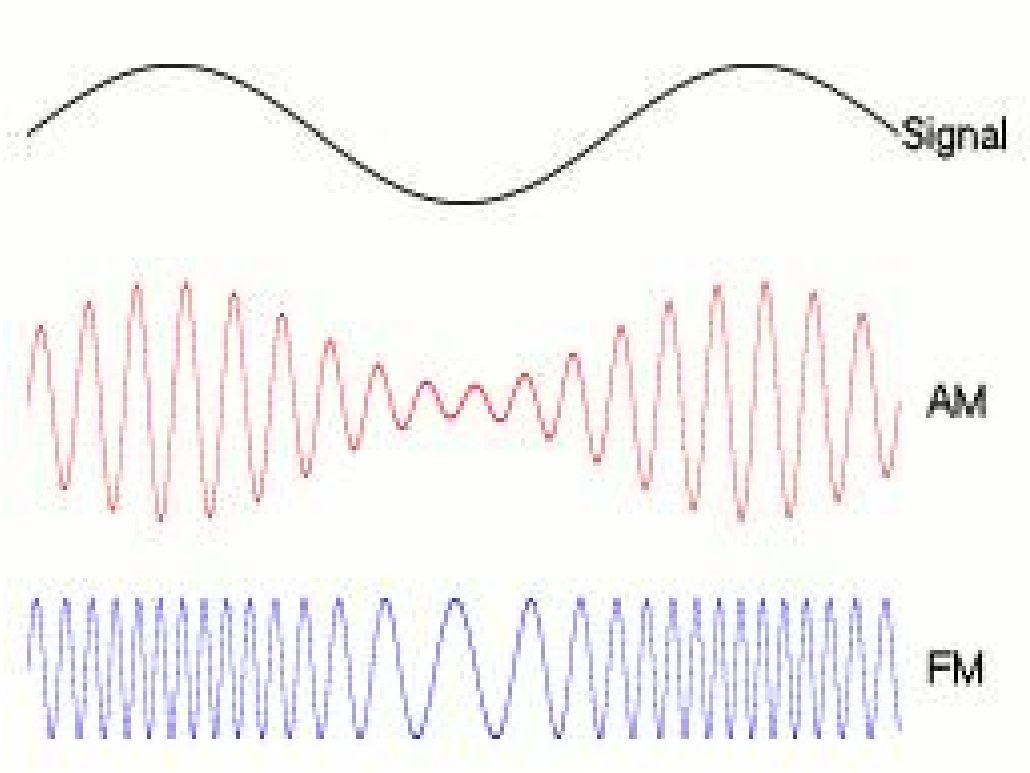
Ex : Phase modulation

Base Télécom
Chaîne de transmission

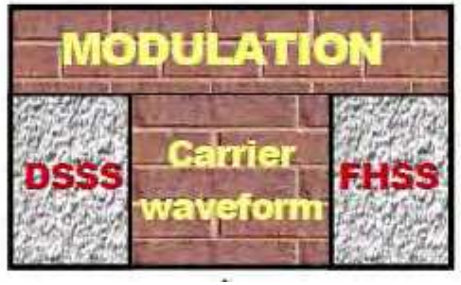


- Modulation:

- Before, it was analog … like AM/FM radios



Base Télécom
Chaîne de transmission



- Modulation:

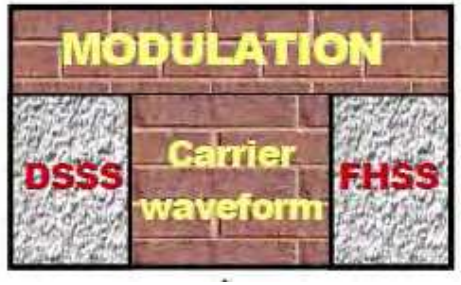
- Then digital … but still on a « carrier » = single frequency $e^{i\omega t}$

4 « best » Choices to converts 0/1 bits into « analog » signal:

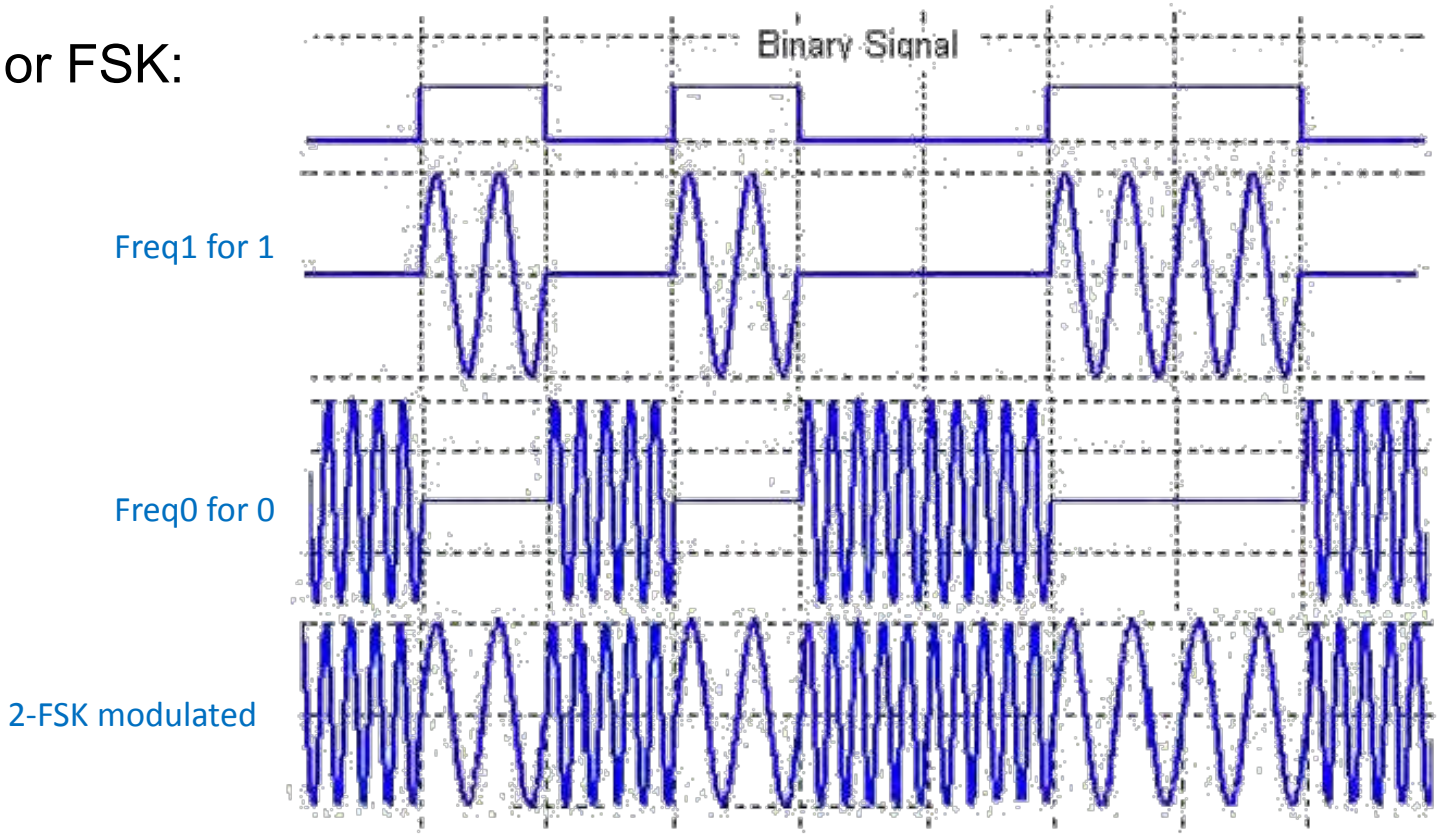
- The uses of phases – Phase Shift Keying or PSK
- The uses of different frequencies – Frequency Shift Keying or FSK
- The uses of different amplitudes – Amplitude Shift Keying or ASK
- The uses of amplitudes and phases combination – Quadrature Amplitude Modulation or QAM

Base Télécom
Chaîne de transmission

- Modulation:



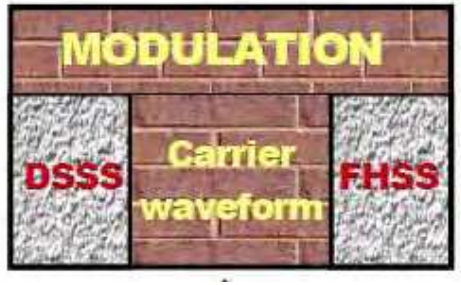
- Frequency Shift Keying or FSK:



AIRBUS

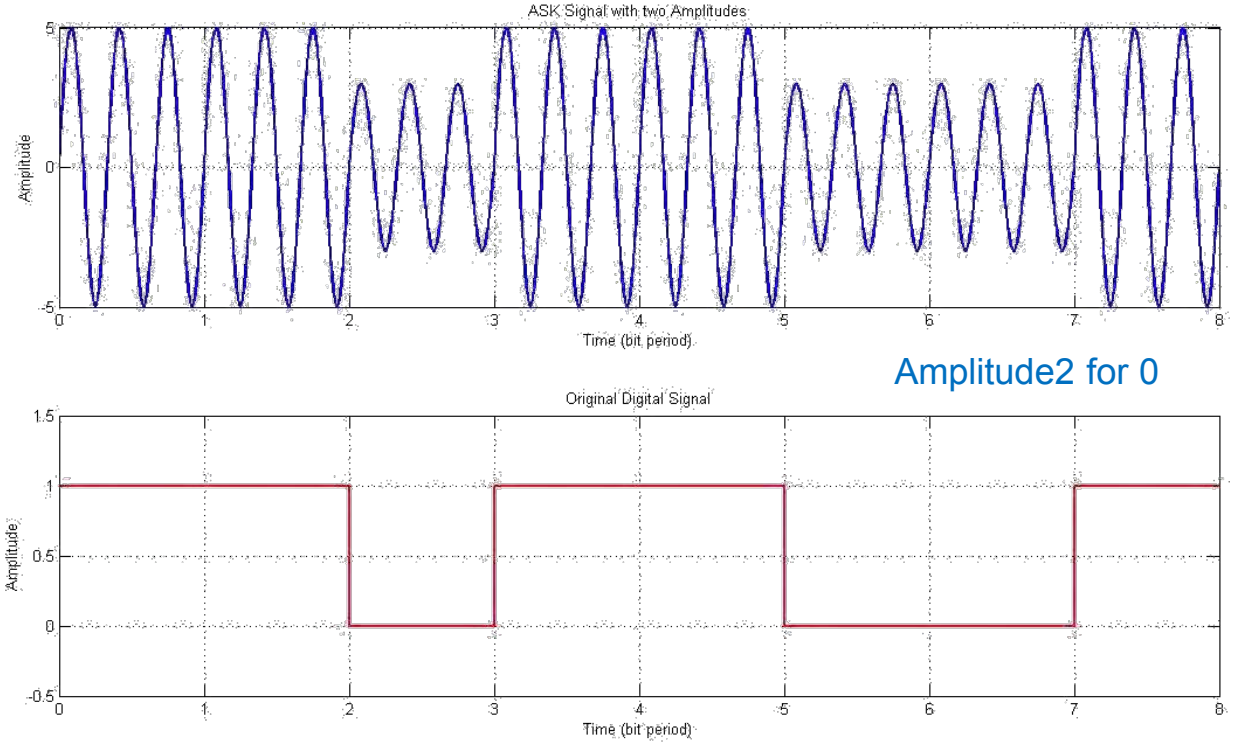
Base Télécom
Chaîne de transmission

- Modulation:



- Amplitude Shift Keying or ASK: $\underline{A} \cdot e^{i\omega t}$

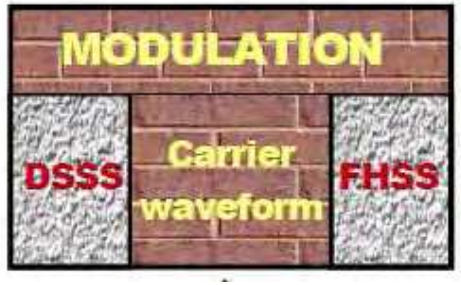
Amplitude1 for 1



Amplitude2 for 0

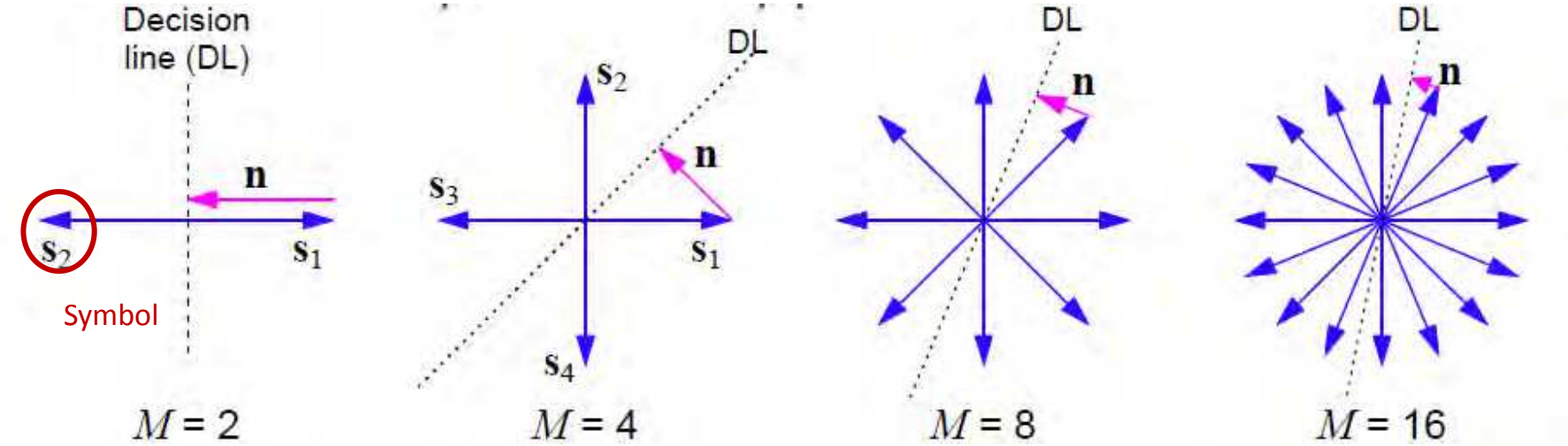
AIRBUS

Base Télécom
Chaîne de transmission



- Modulation:

- Phase Shift Keying or PSK: $A \cdot e^{i\omega t+\underline{\varphi}}$

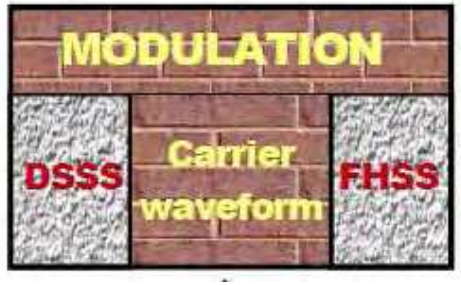


BPSK QPSK 8-PSK

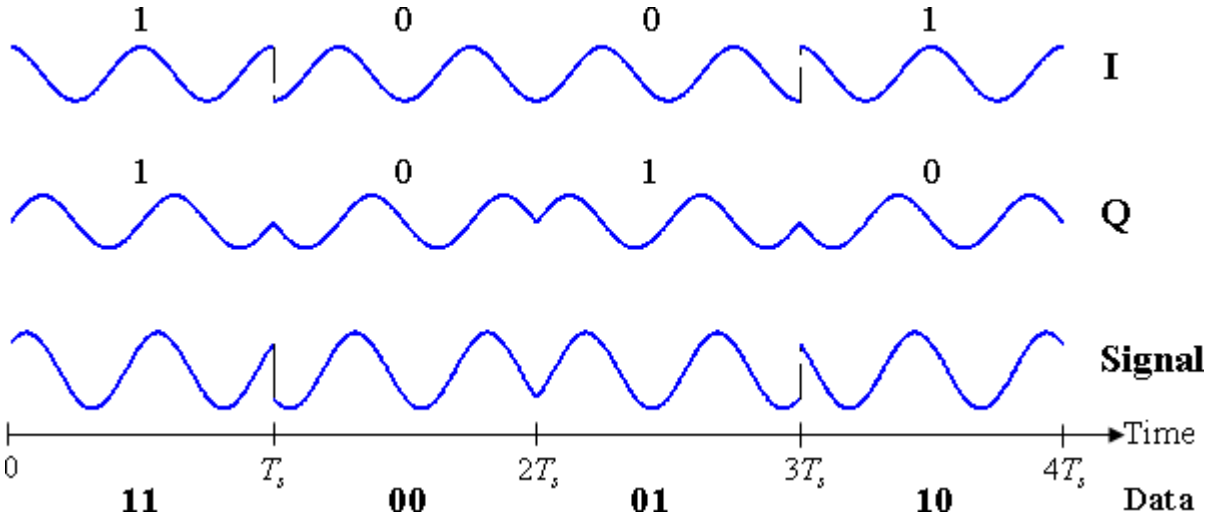
AIRBUS

Base Télécom
Chaîne de transmission

- Modulation:



- Phase Shift Keying or PSK: $A \cdot e^{i\omega t+\underline{\varphi}}$

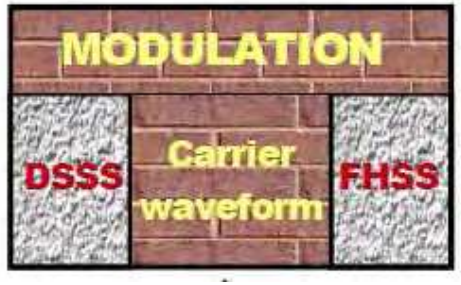


$T_s = \frac{1}{f_s},$ Symbol duration

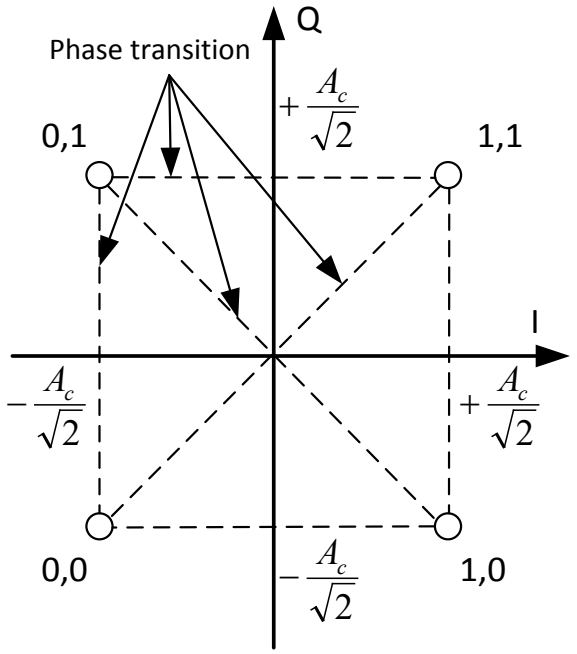
QPSK timing diagram

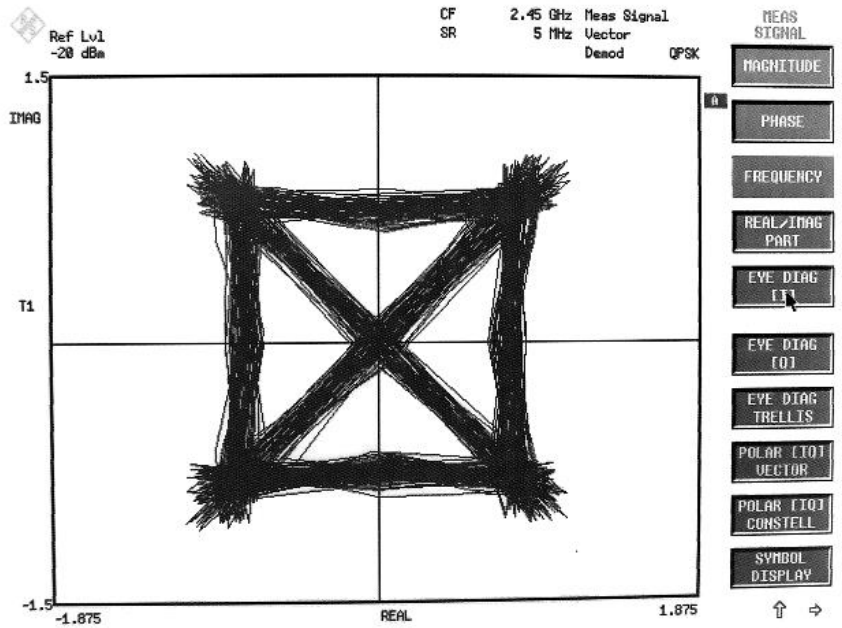
Base Télécom
Chaîne de transmission

- Modulation:



- Phase Shift Keying or PSK: $A \cdot e^{i\omega t+\underline{\varphi}}$



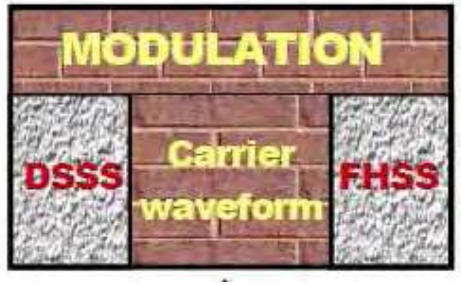


[QPSK constellation]

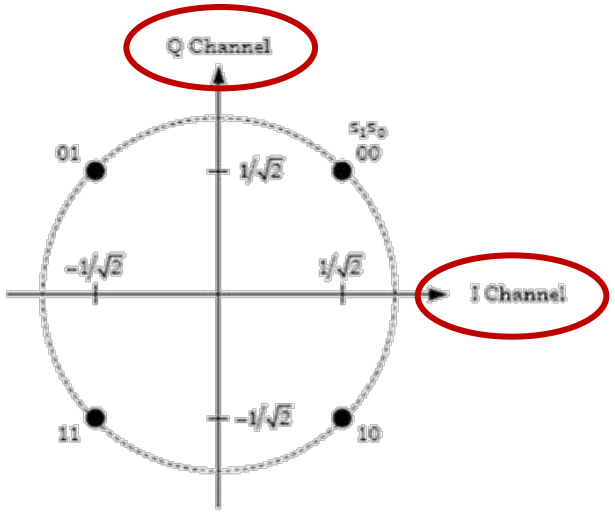
AIRBUS

Base Télécom
Chaîne de transmission

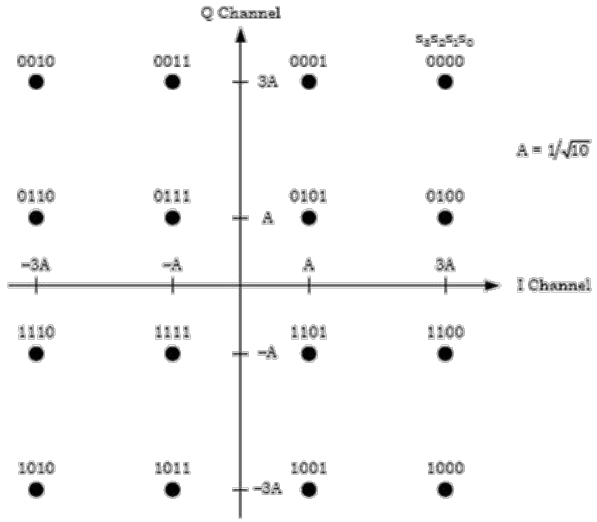
- Modulation:



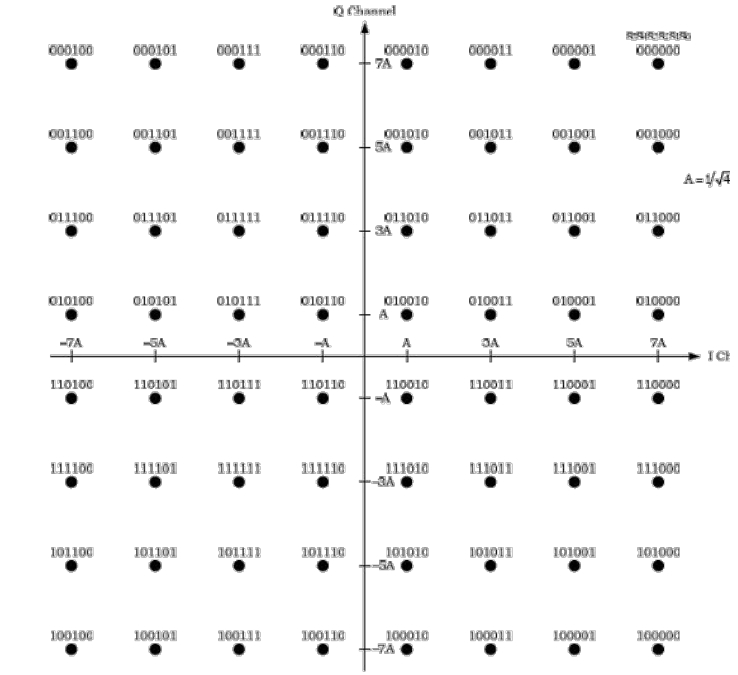
- Quadrature Amplitude Modulation: $\underline{A} \cdot e^{i\omega t+\underline{\varphi}}$



QPSK or 4-QAM



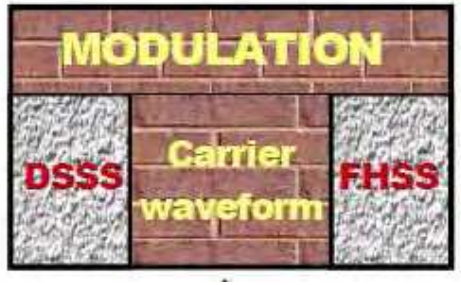
16-QAM



64-QAM

AIRBUS

Base Télécom
Chaîne de transmission



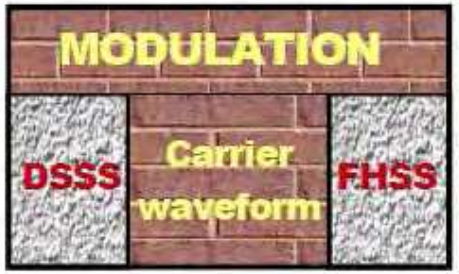
- Modulation:

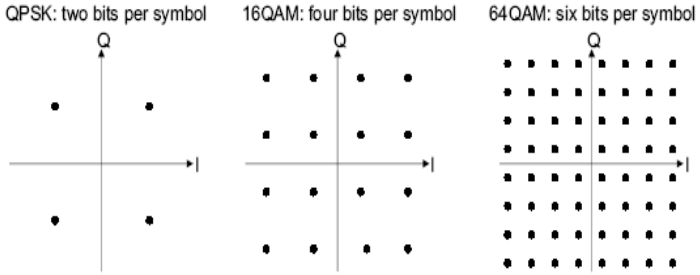
- Options:
  - DSSS
  - FHSS

Chap. Sécurisation

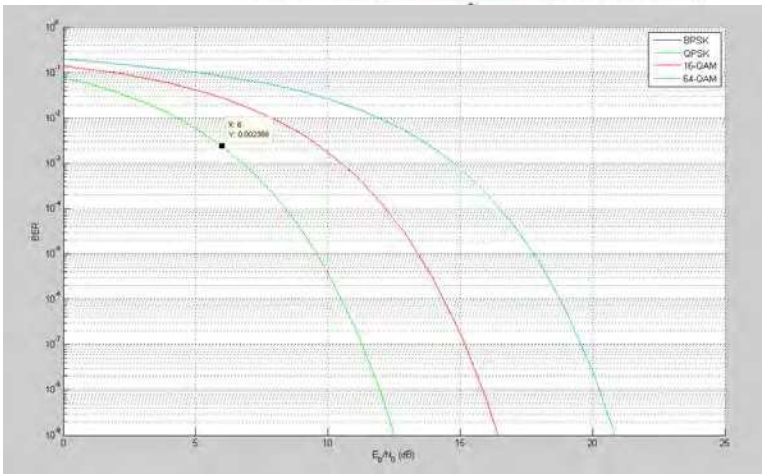
Base Télécom
Chaîne de transmission

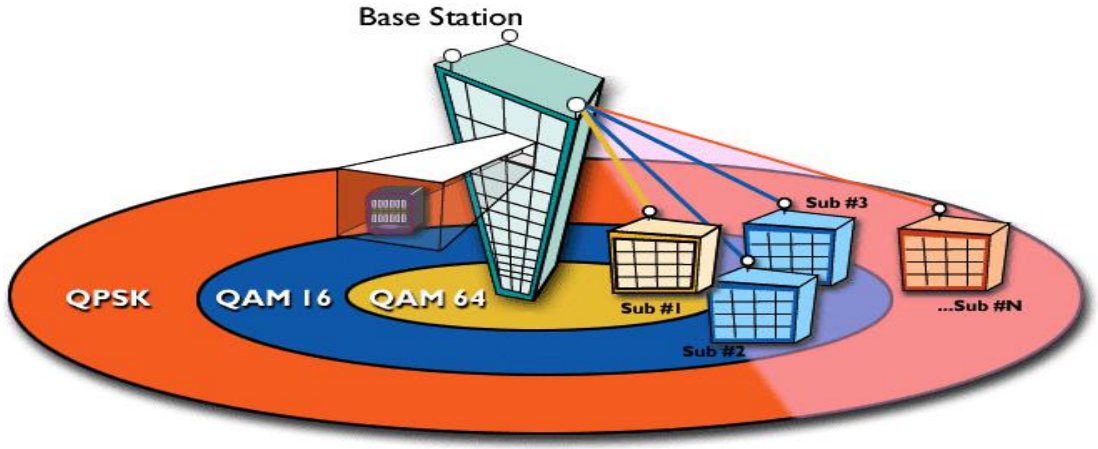
- Modulation:





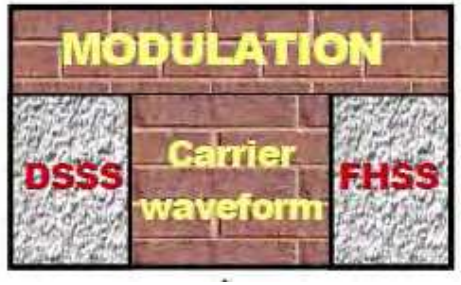
- Link adaptation:



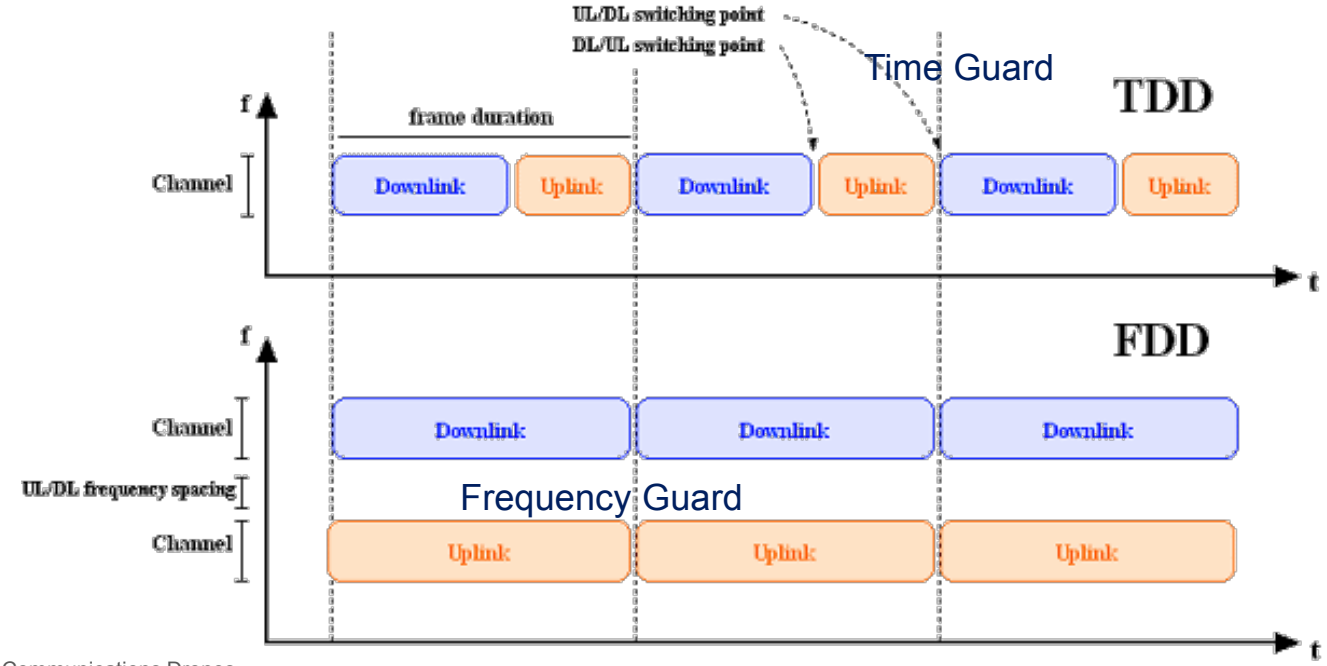


AIRBUS

Base Télécom
Chaîne de transmission

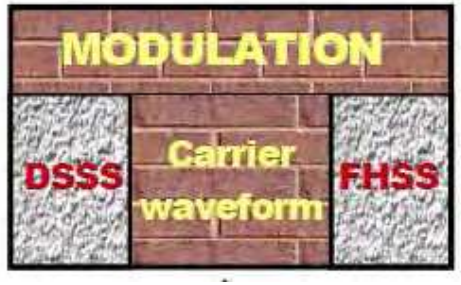


- Modulation: Duplexing
- Uplink / Downlink sharing of the channel = duplexing:
  2 main solutions:
  - 2 frequencies one for Uplink, one for Downlink = **FDD**
  - Time share of the radio channel: one time for Uplink, one time for Downlink = **TDD**



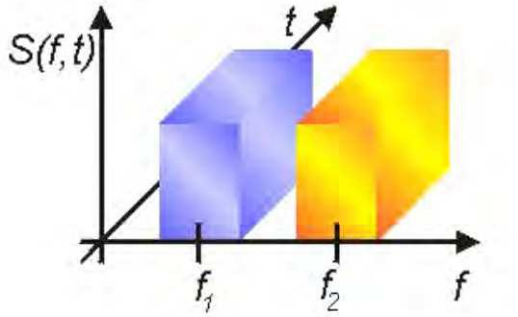
AIRBUS

Base Télécom
Chaîne de transmission



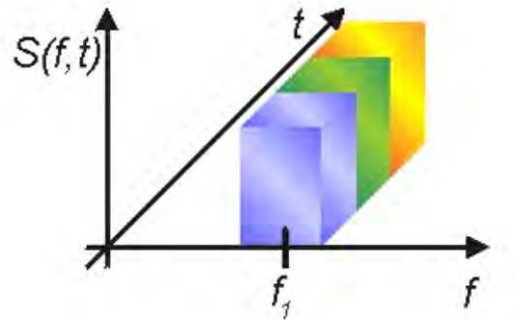
- Modulation: Multiple Access Techniques

FDMA
Frequency Division Multiple Access



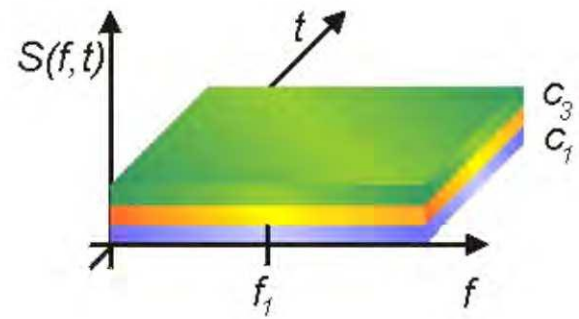
Organized Access with different frequencies for the different users

TDMA
Time Division Multiple Access



Organized Access with time share between users

WCDMA
Wideband Code Division Multiple Access

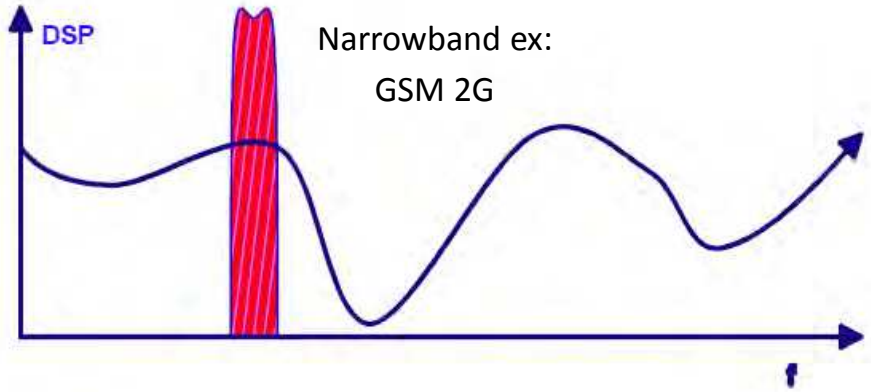


Organized Access with code division between users

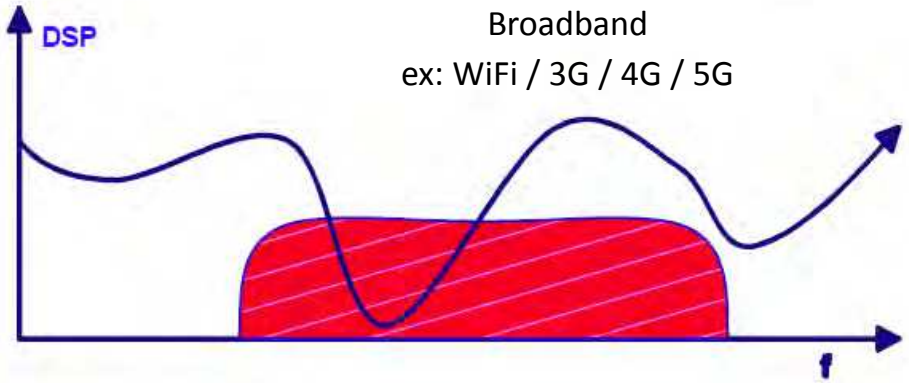
AIRBUS

Base Télécom
Chaîne de transmission

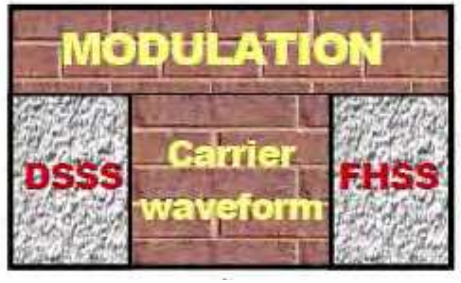
- Modulation: OFDM

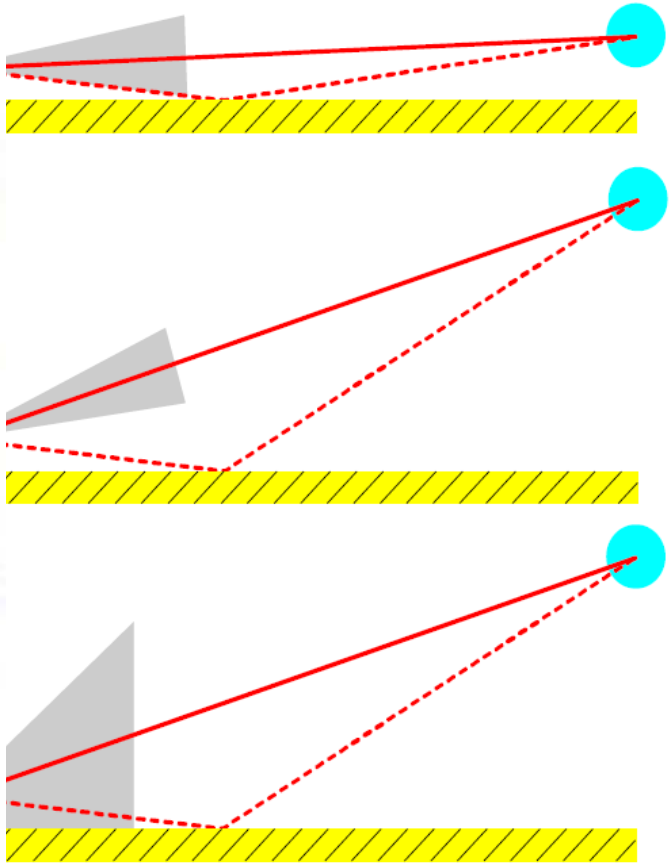


Narrowband ex:
GSM 2G



Broadband
ex: WiFi / 3G / 4G / 5G





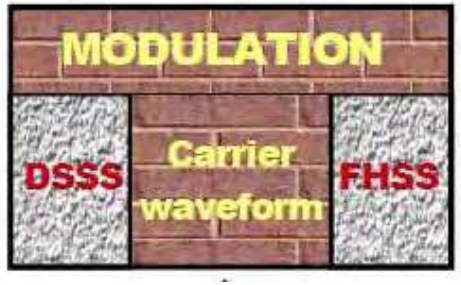
Cas 1
Longue portée point à point:
Sélectivité moyenne
origine atmosphérique

Cas 2
Courte portée point à point:
Pas de sélectivité

Cas 3
BROADCAST:
Sélectivité intense
origine réflexion du sol

AIRBUS

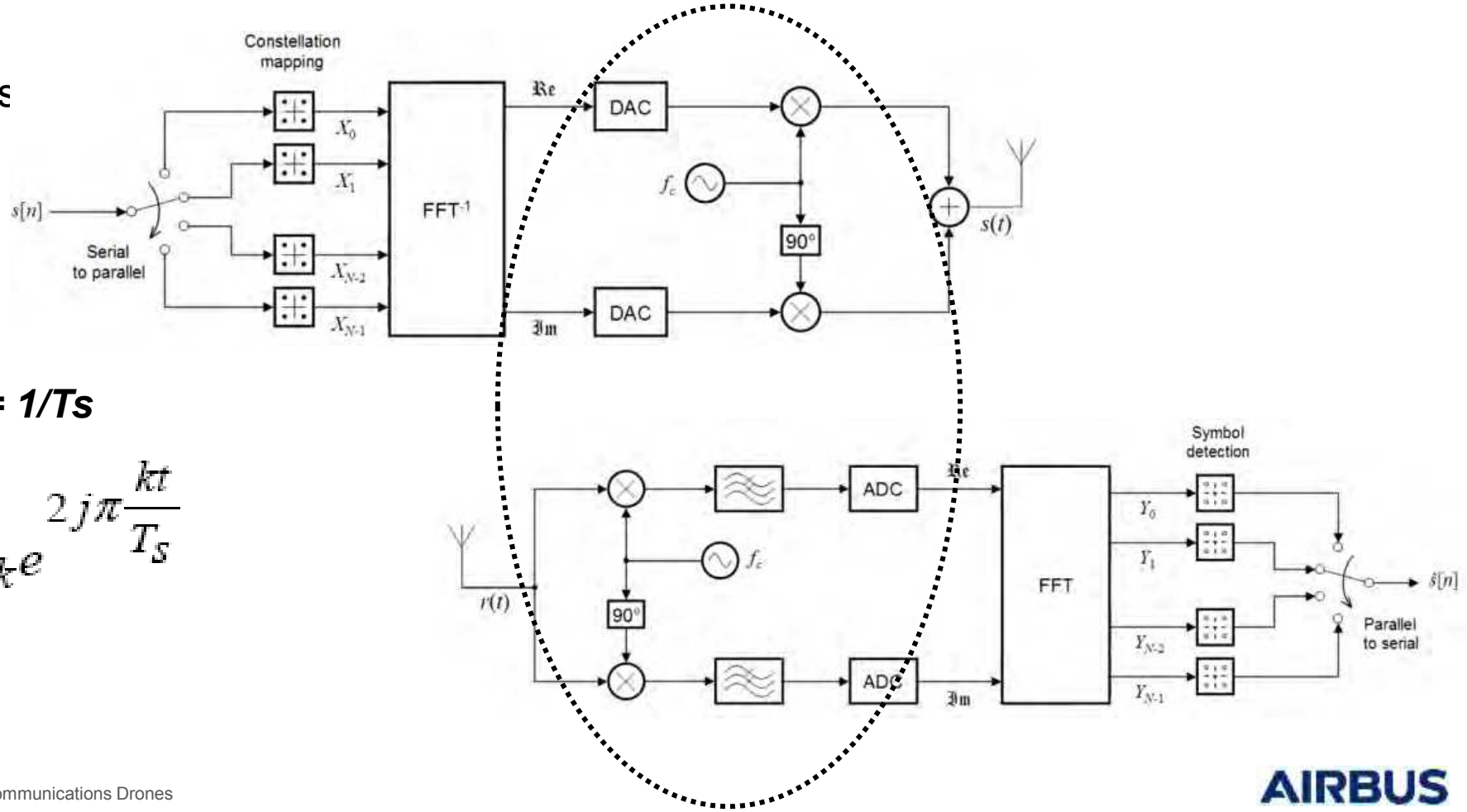
Base Télécom
Chaîne de transmission



- Modulation: OFDM

Somme de porteuses modulées

$$s(t) = \sum_{k=0}^{N-1} c_k e^{2j\pi f_k t}$$



- Choix ***fk = f0 + k*Δ*f*** and Δ ***f = 1/Ts***

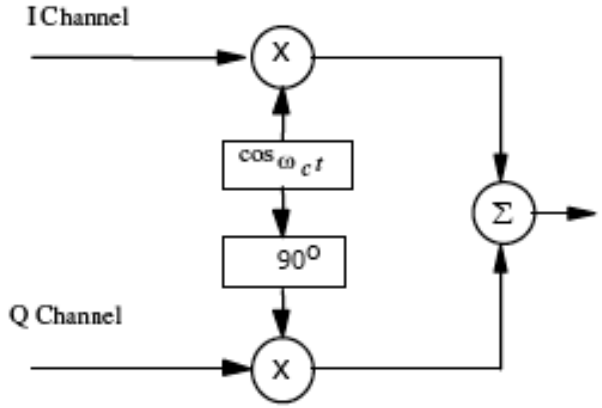
$$s(t) = e^{2j\pi f_0 t} \sum_{k=0}^{N-1} c_k e^{2j\pi \frac{kt}{T_s}}$$

AIRBUS

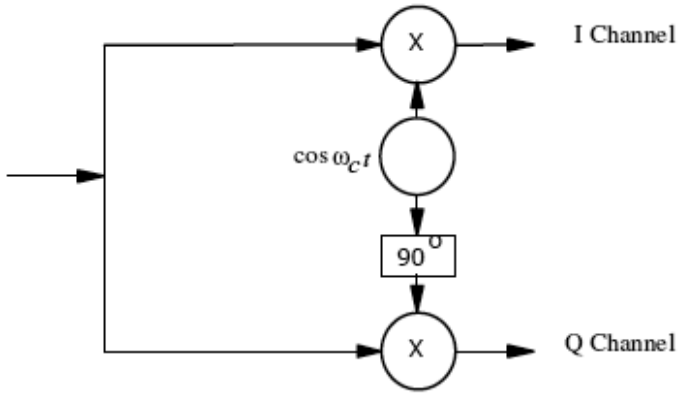
Base Télécom
Chaîne de transmission

- Adaptation to propagation medium:

- Converts the electrical waveform to an electromagnetical wave by the mean of:
  - *Quadrature modulator / demodulator*



Quadrature Modulator



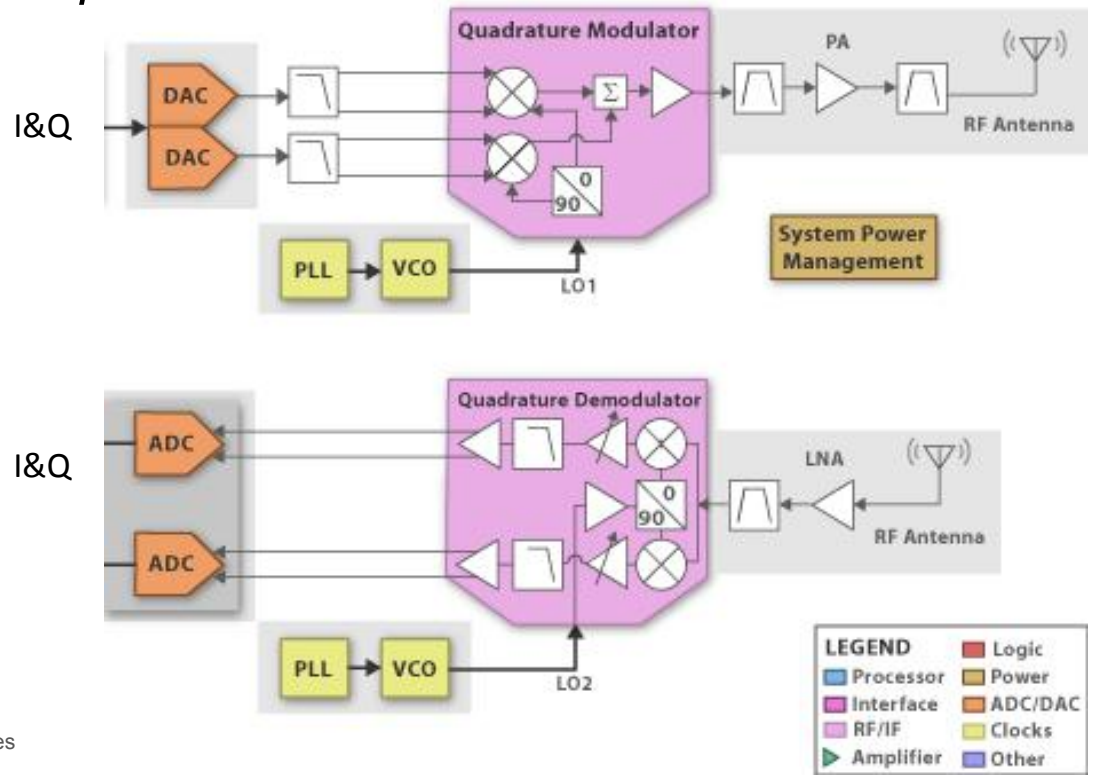
Quadrature Demodulator

AIRBUS

Base Télécom
Chaîne de transmission

- Adaptation to propagation medium:

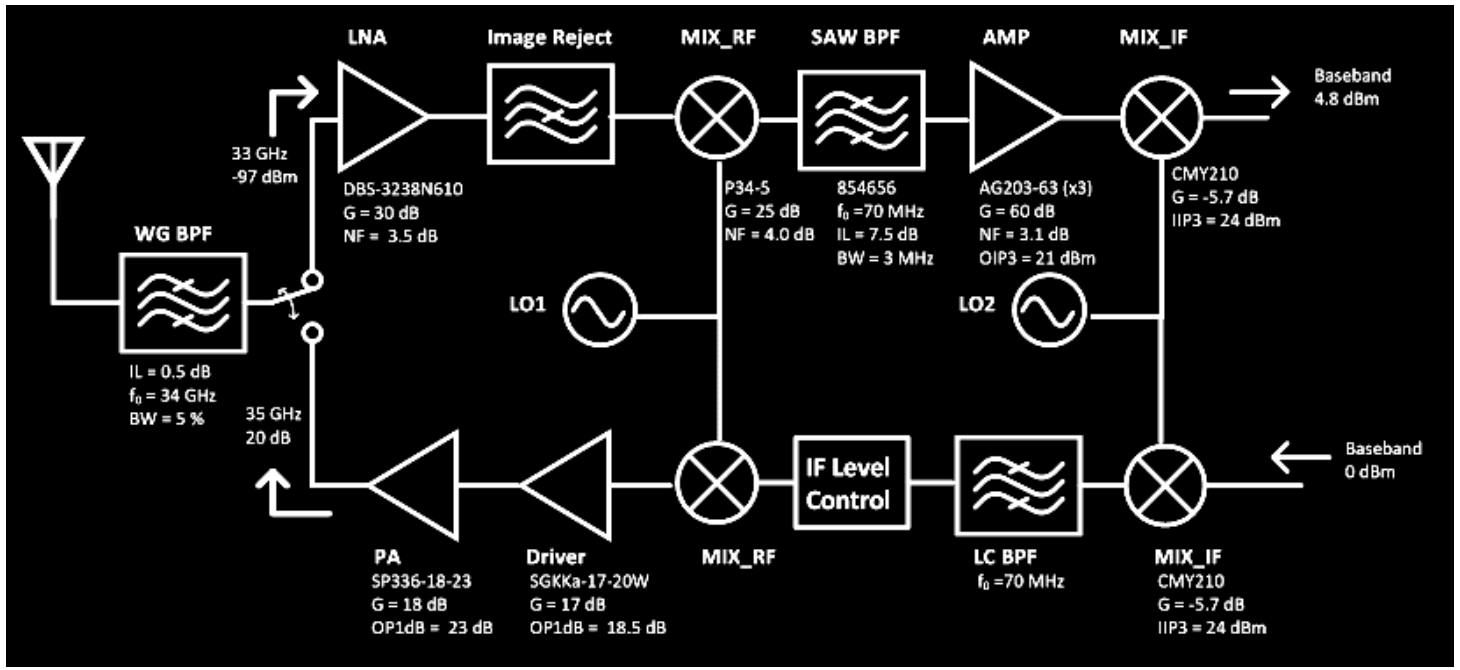
- Converts the electrical waveform to an electromagnetical wave by the mean of:
  - *Microwave electronics or Radio Frequencv electronics*
  - *Antenna*



Base Télécom
Chaîne de transmission

- Adaptation to propagation medium:

- Converts the electrical waveform to an electromagnetical wave by the mean of:
  - *Microwave electronics or Radio Frequency electronics*
  - *Antenna*



AIRBUS

Base Télécom
Chaîne de transmission

- Propagation medium or Channel:

- Space between the emitter and the receiver

- Home for a **link budget** !

$$P_{received} = P_{emitted} + Gain_{emission} + Gain_{reception} - Losses - PathLoss$$

Base Télécom
Chaîne de transmission

- Propagation medium or Channel: terminology
  - **BER** or Bit-Error Rate, for measurement of performance
  - **SNR** (S/N) or Signal to Noise Ratio: $SNR = (Signal\ Power\ S)/(Noise\ Power\ N)$
  - **SINR** or Signal to Interferences + Noise Ratio:

$$SINR = (Signal\ Power\ S)/(Noise\ Power\ N + Interferences\ Power\ I)$$

  - **Eb/No** or Energy per Bit to Noise power spectral Density & Es or Energy per Symbol :

$$SNR = Eb/N\_0 \cdot f\_b/B \quad \& \quad E\_s/N\_0 = E\_b/N\_0 \ \log\_2 M$$

  - **B** is the channel bandwidth / fb is the channel data rate
    M is the number of modulation symbols

Base Télécom
Chaîne de transmission

- Propagation medium or Channel: link budget

Link Budget :

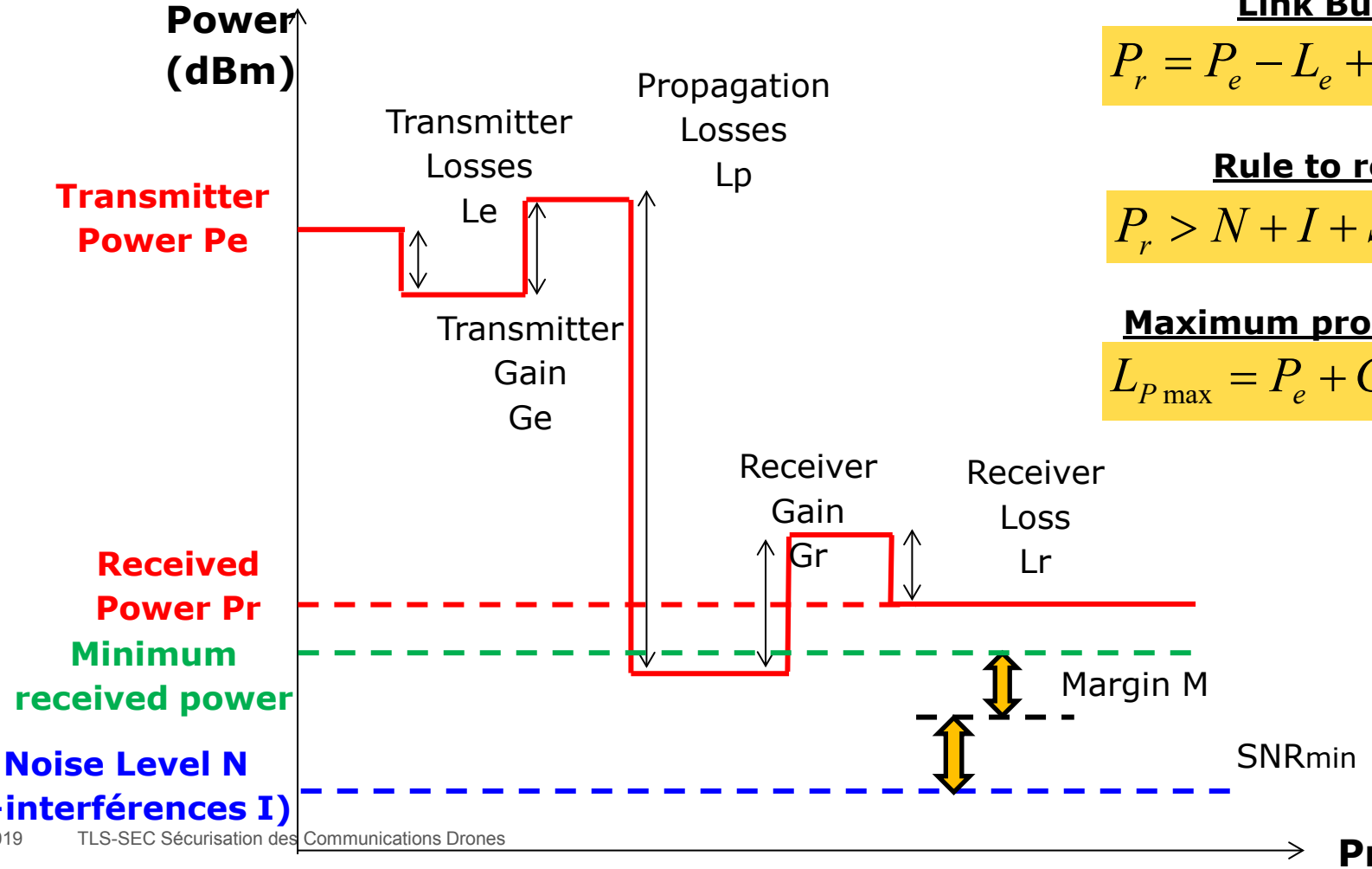
$$P_r = P_e - L_e + G_e - L_p + G_r - L_r$$

Rule to respect :

$$P_r > N + I + SNR_{\min} + M$$

Maximum propagation losses :

$$L_{P\max} = P_e + G_e - L_e - P_{r\min} - L_r + G_r$$

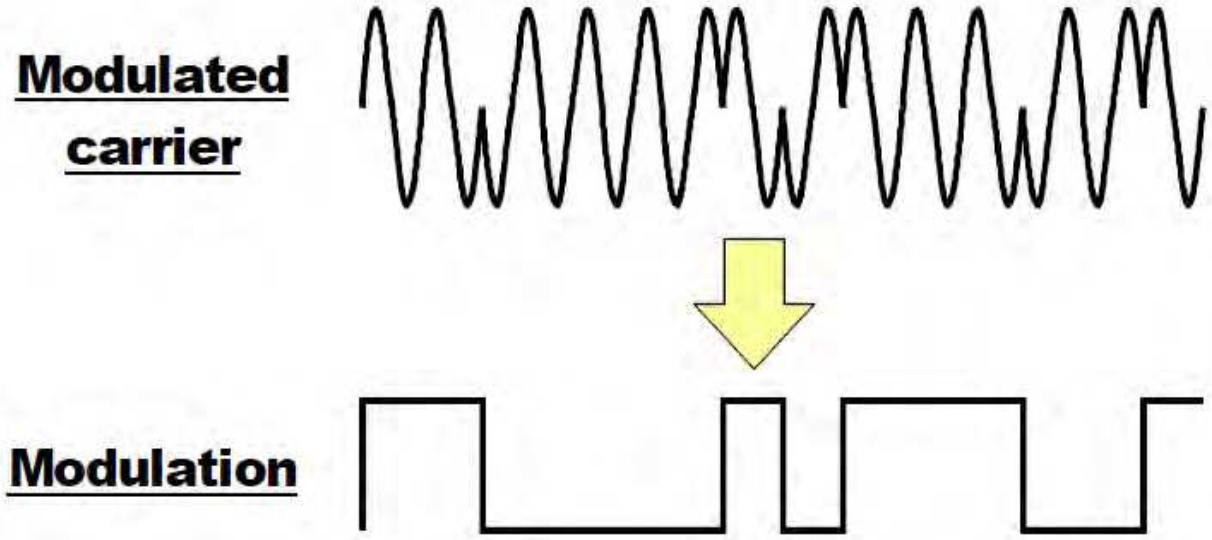


AIRBUS

Base Télécom
Chaîne de transmission

- Demodulation:

- Converts the signal on a carrier into an information signal

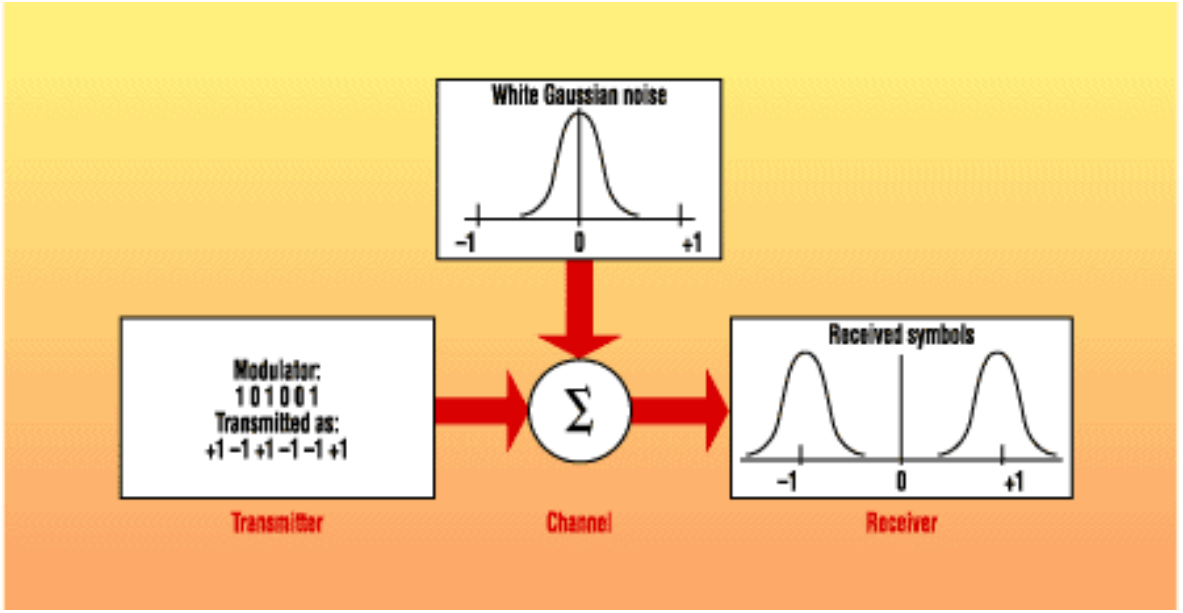


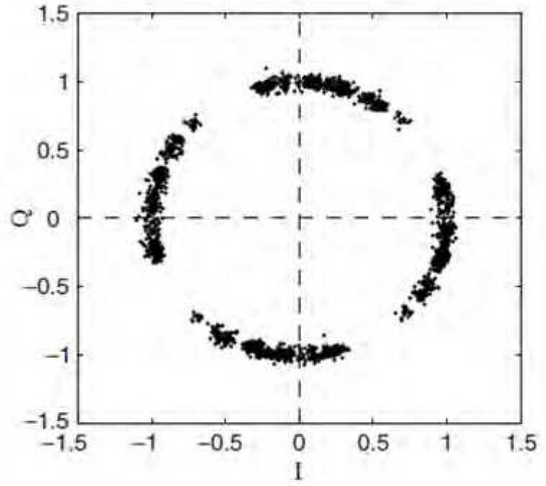
… But that is not so easy, as the propagation channel is the troublemaker in-between !

Base Télécom
Chaîne de transmission

- Demodulation:

- Apart the amplitude problem, the propagation channel introduces random phase shifts AND noise



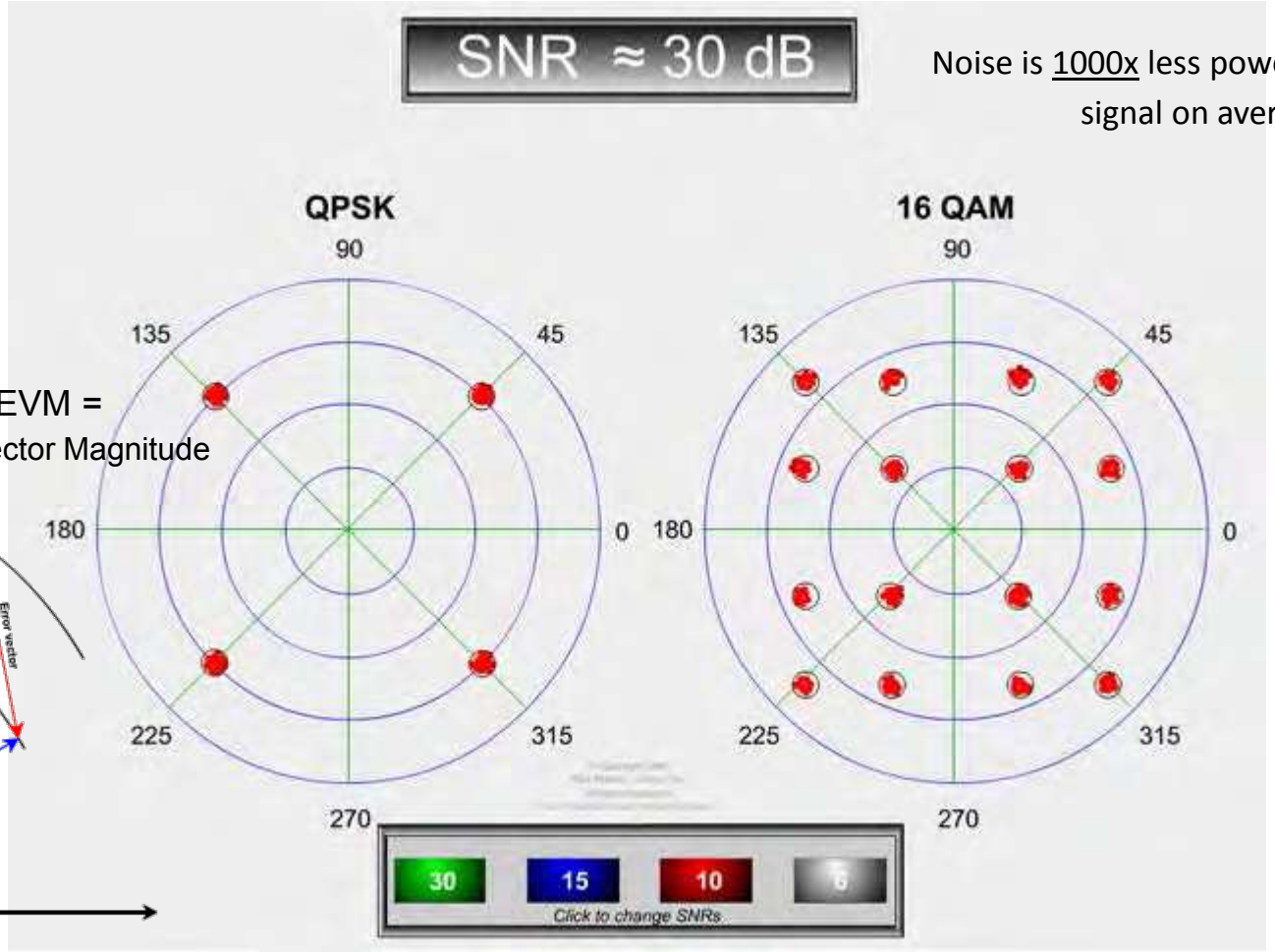


Effect of Phase Noise

AIRBUS

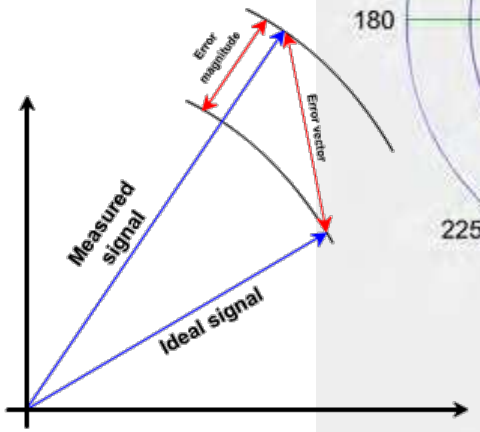
Base Télécom
Chaîne de transmission

- Demodulation:



Noise is 1000x less powerfull than the signal on average

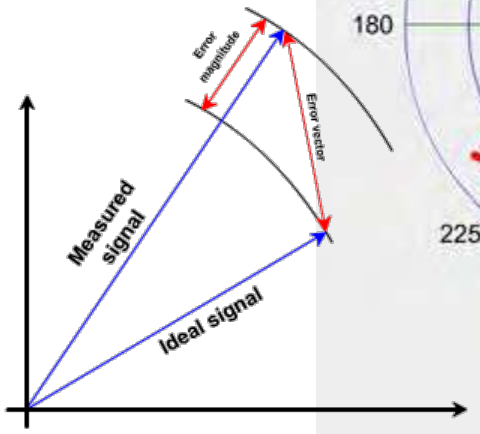
EVM =
Error Vector Magnitude

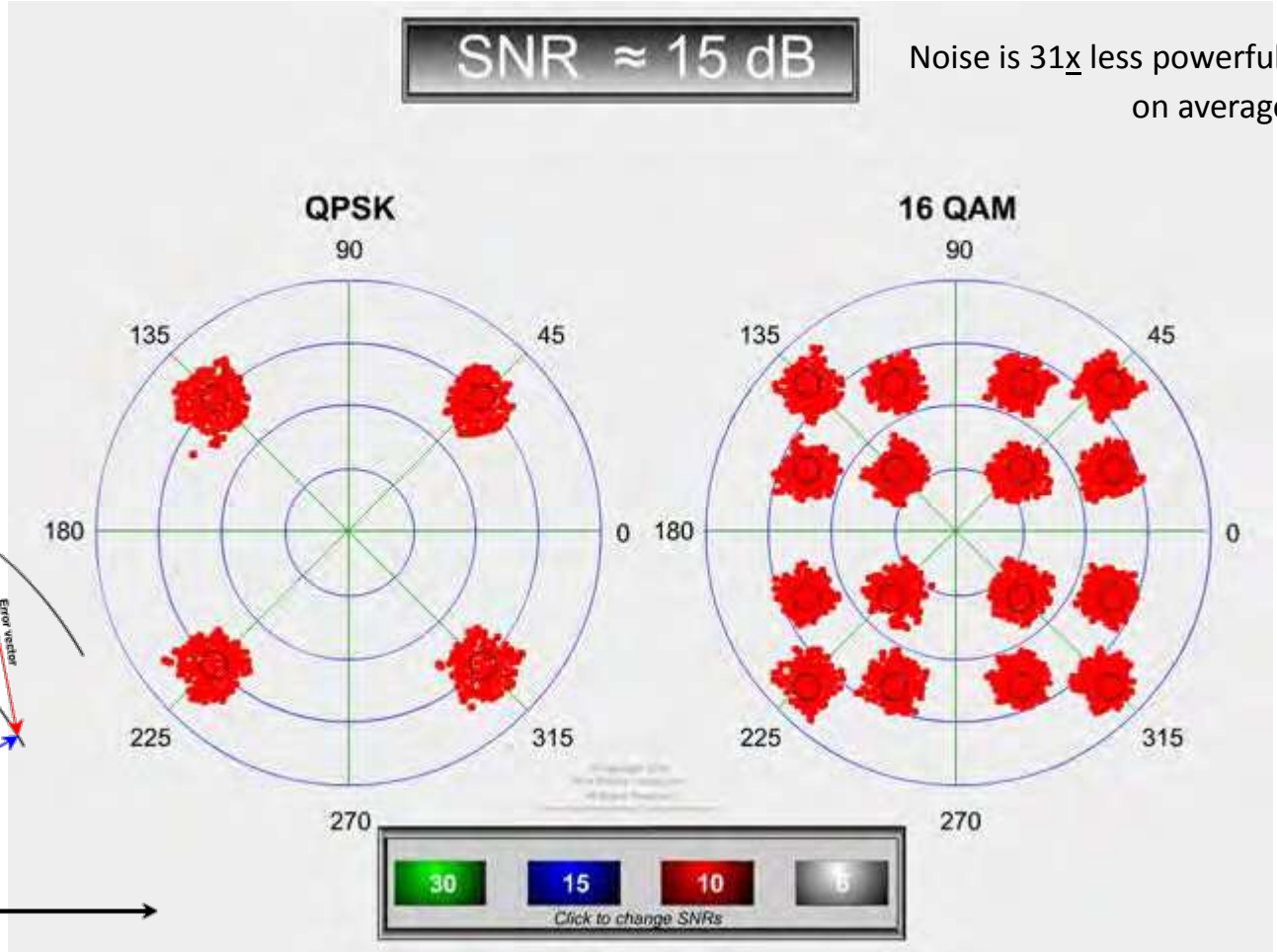


AIRBUS

Base Télécom
Chaîne de transmission

- Demodulation:



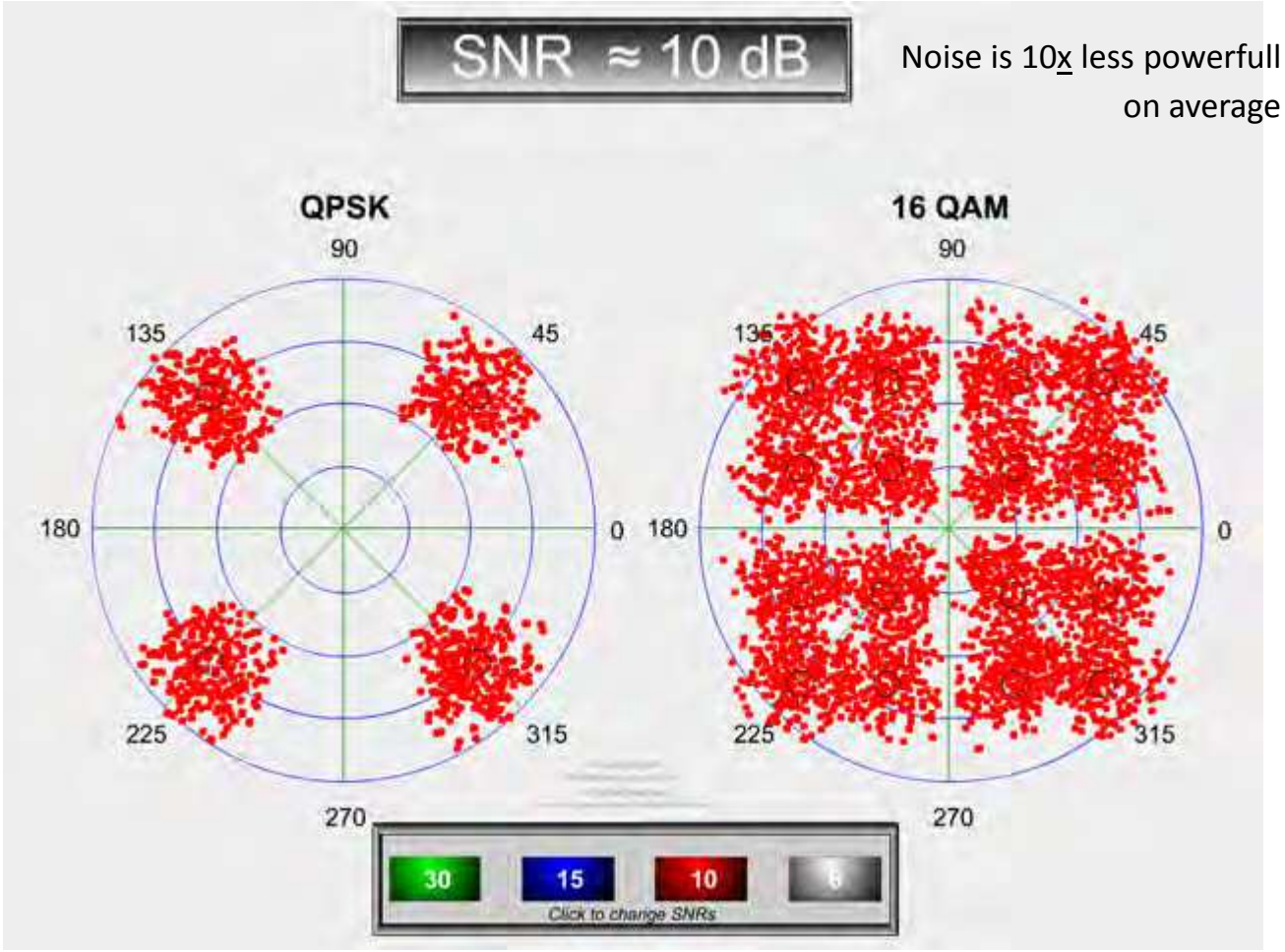


Noise is 31x less powerfull than the signal on average

AIRBUS

Base Télécom
Chaîne de transmission

- Demodulation:

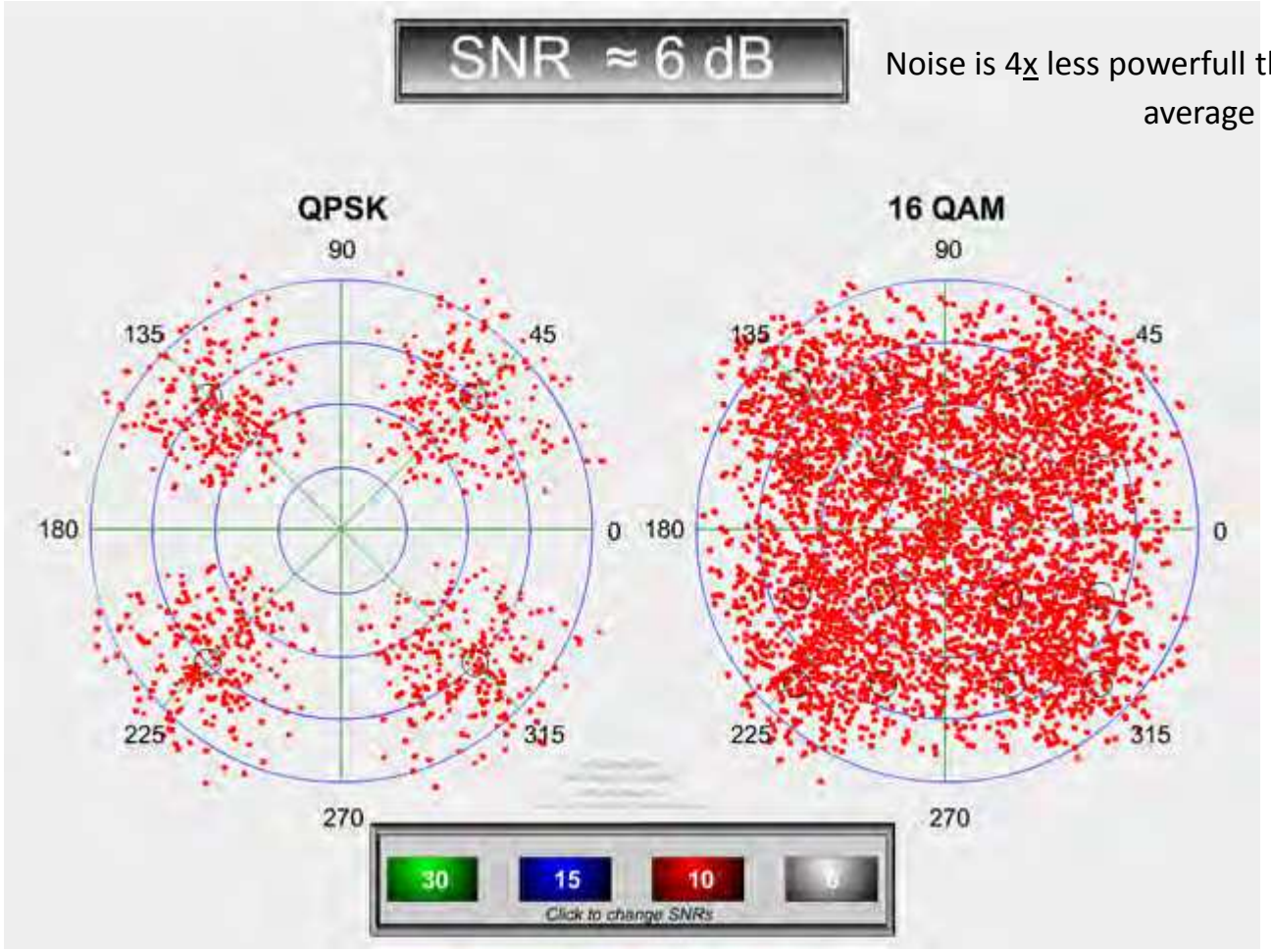


Noise is 10x less powerfull than the signal on average

AIRBUS

Base Télécom
Chaîne de transmission

- Demodulation:

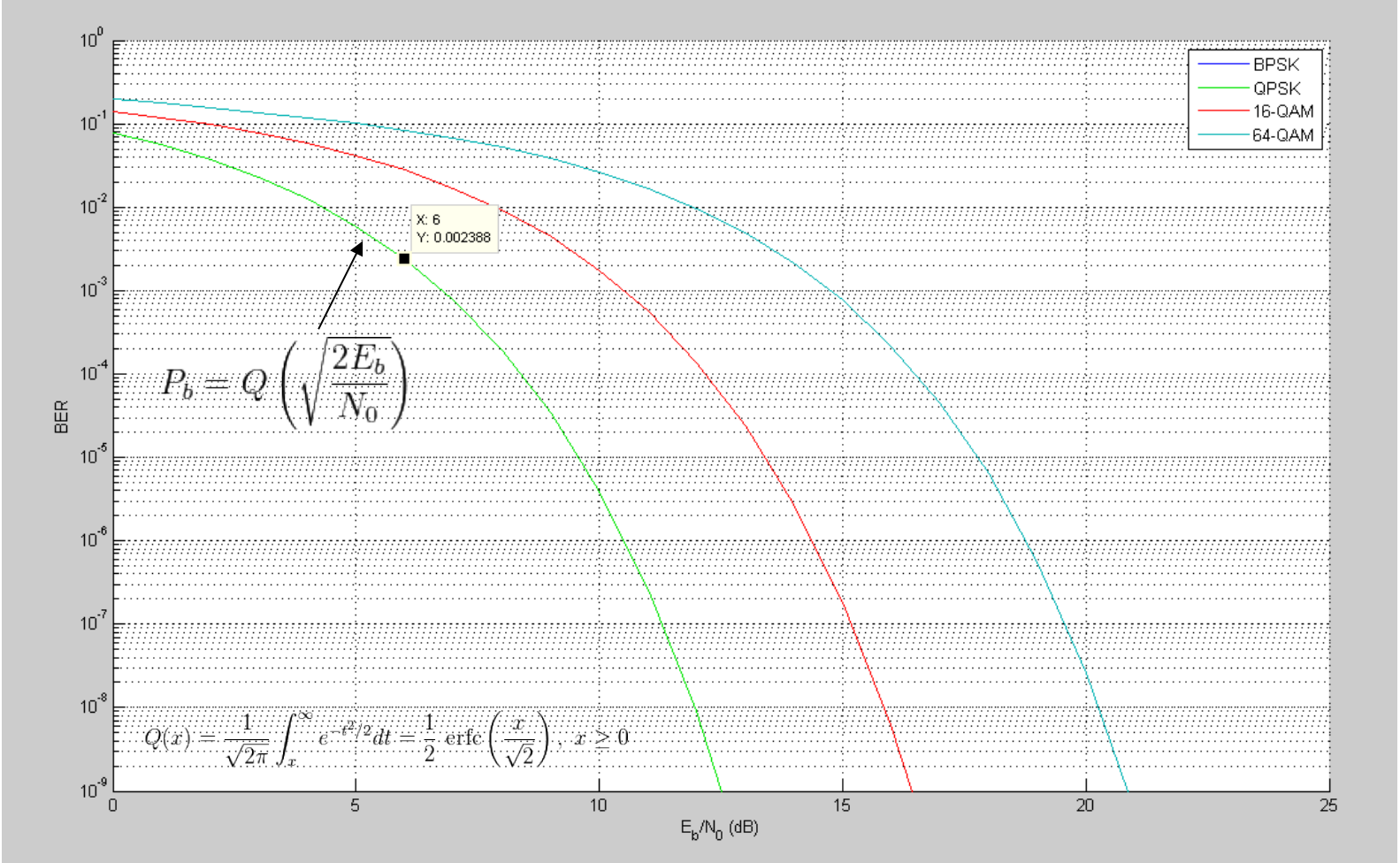


Noise is 4x less powerfull than the signal on average

AIRBUS

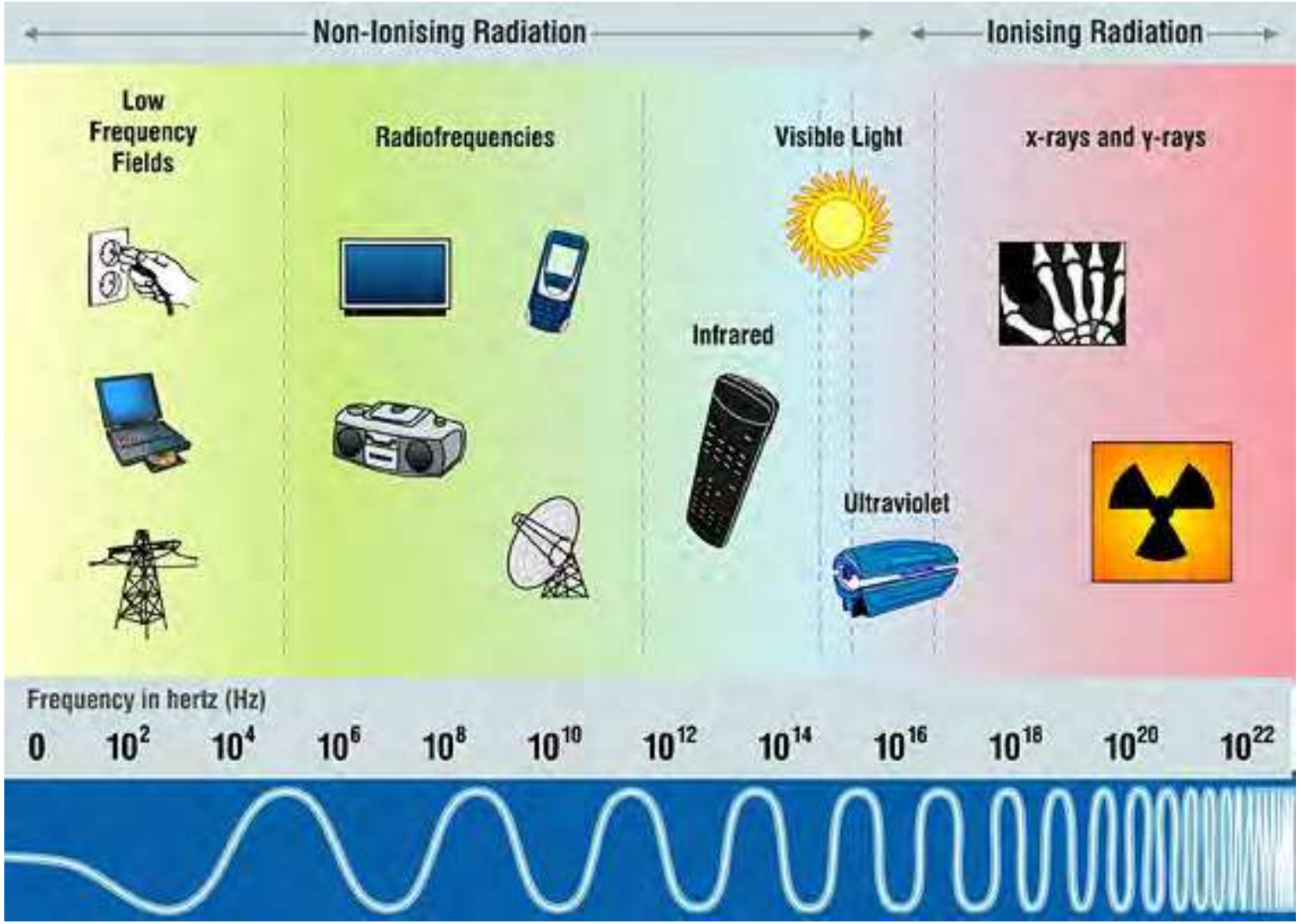
Base Télécom
Chaîne de transmission

- Demodulation: : BER « waterfall » curves



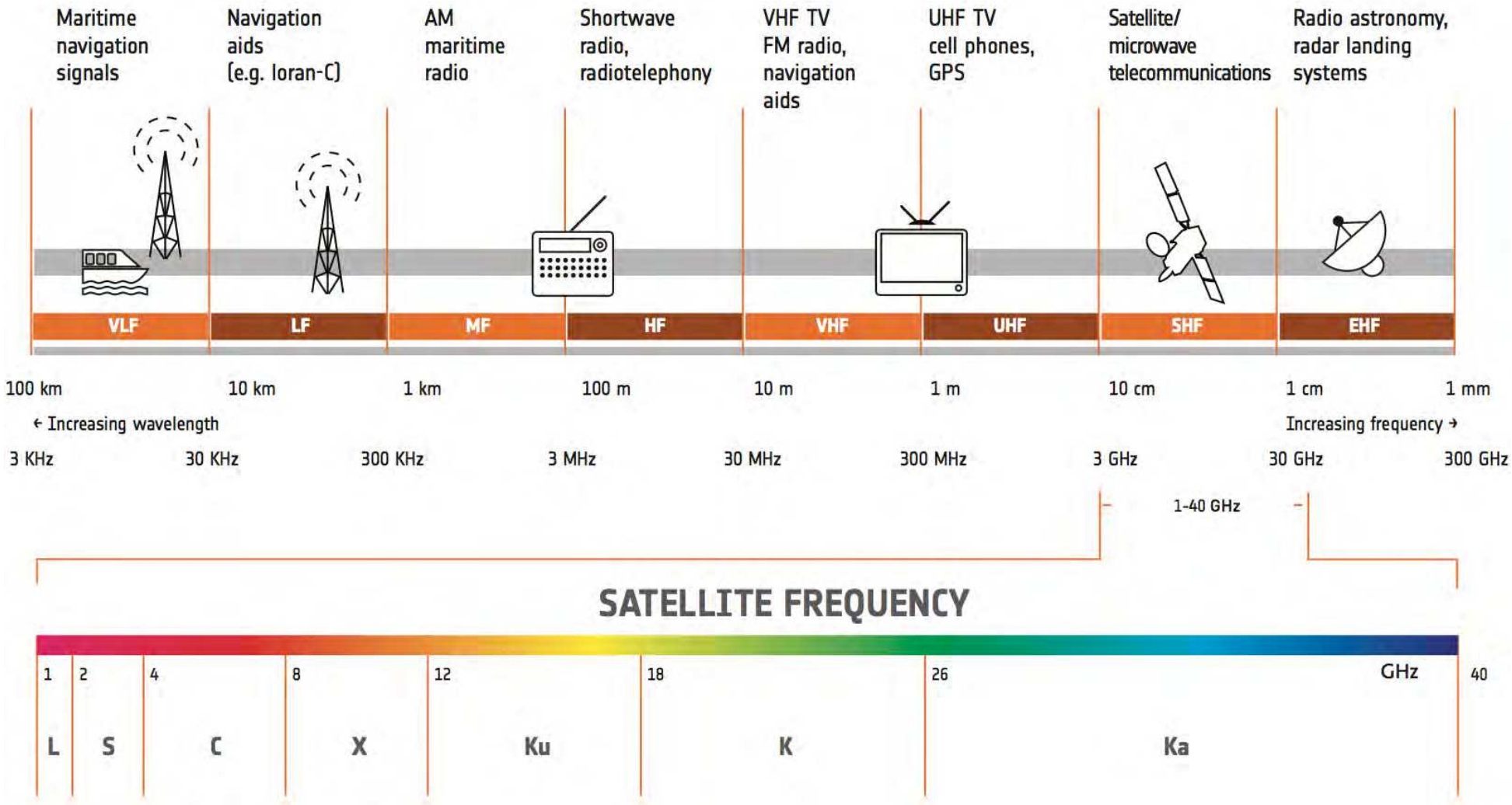
AIRBUS

Base Télécom
Fréquences



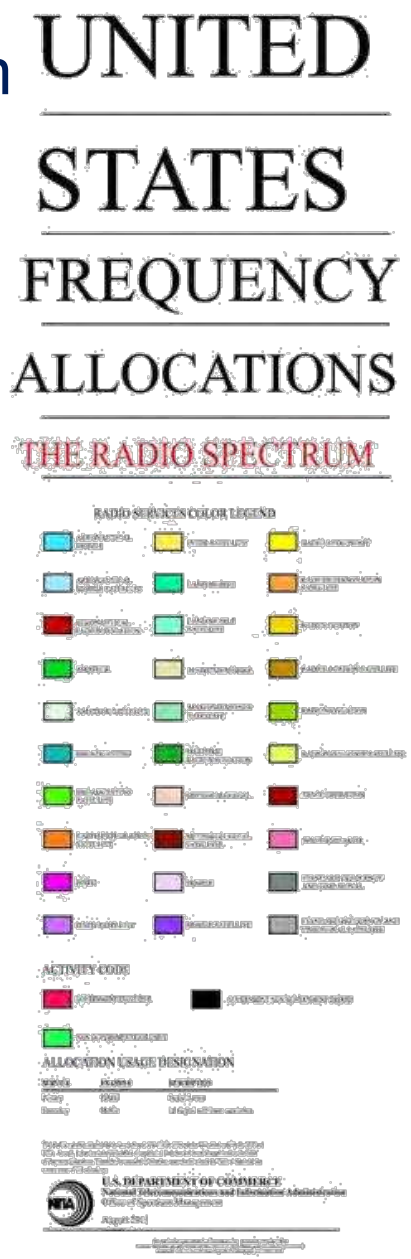
AIRBUS

Base Télécom
Fréquences



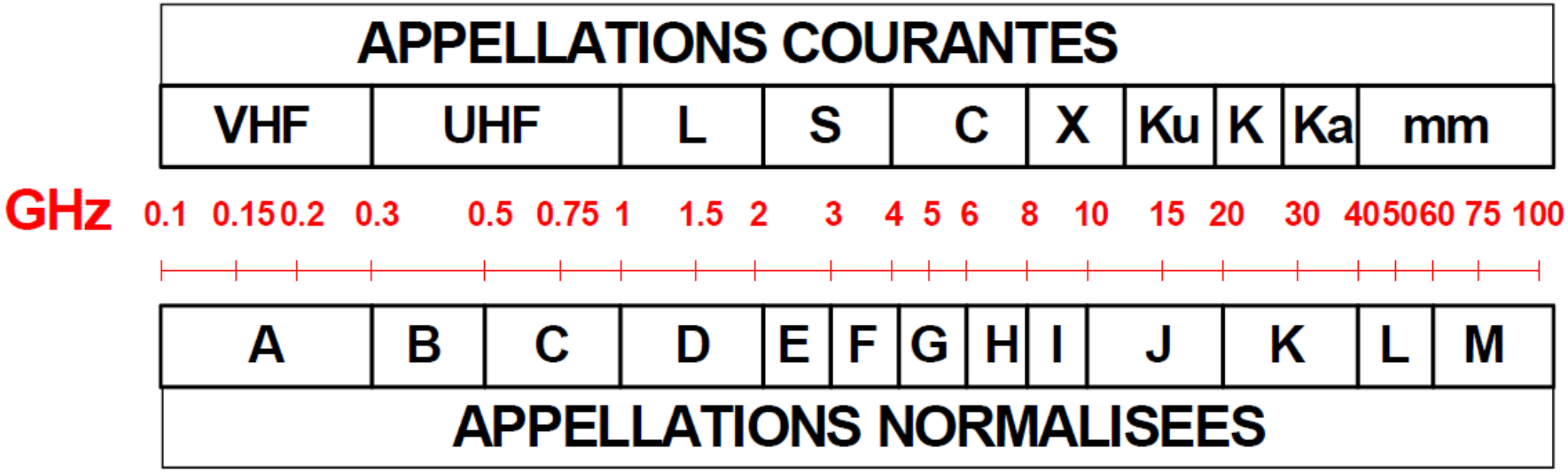
AIRBUS

Base Télécom Fréquences



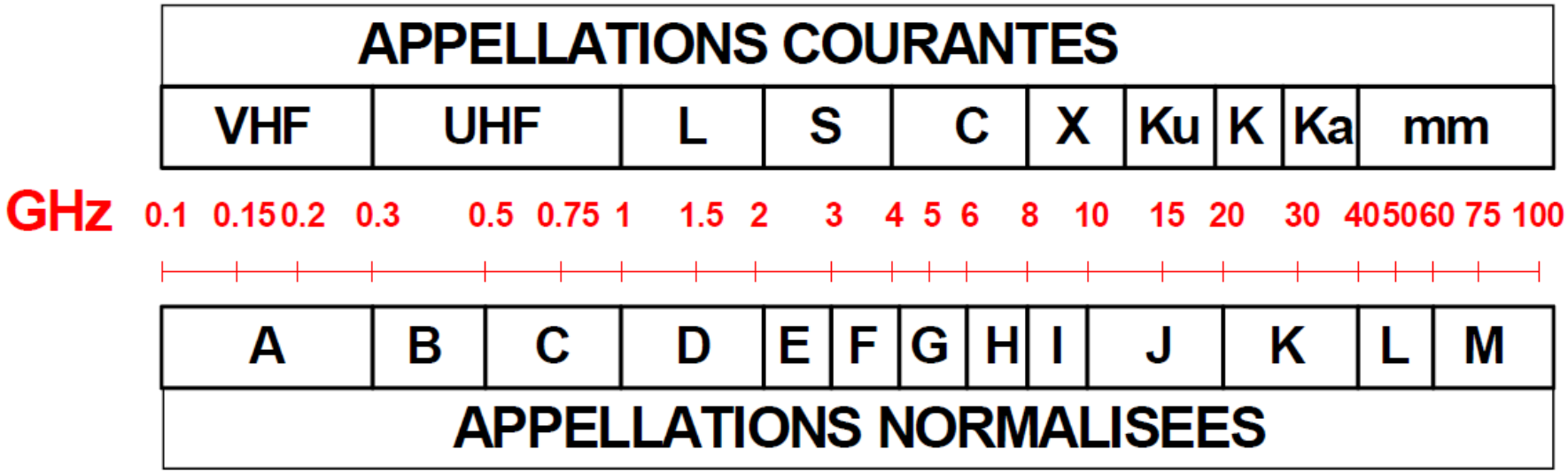
AIRBUS

Base Télécom
Fréquences



- Drones MIL:
  - STANAG 7085 & 4660 & 4606 (antibrouillage) pour les bandes réservées aux UAV (LOS)
    - X interdite en France
    - Ku 14,5-15,25 GHz autorisée en France

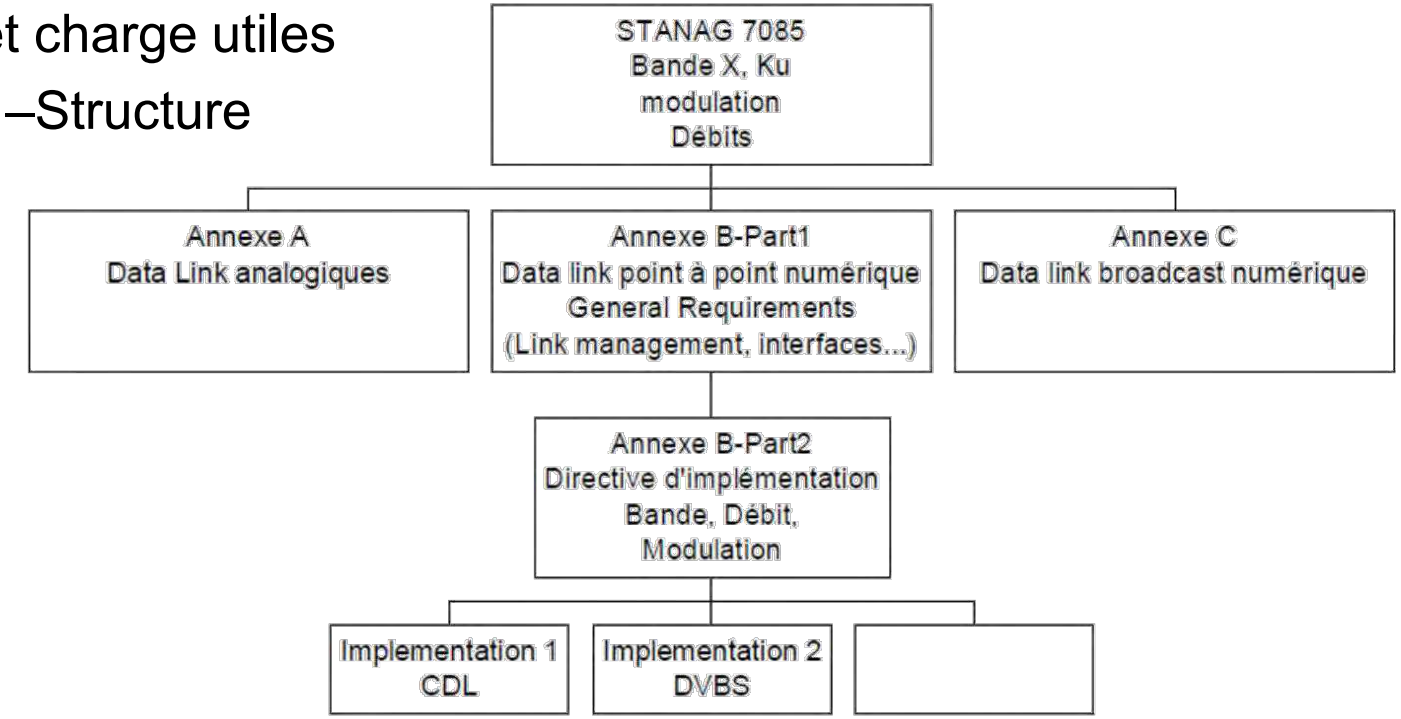
Base Télécom
Fréquences



- Drones Civils: dépend du type de drone professionnel ou non (grand public)
  - **Professionnel:**
    - Bandes non licenciées et 5GHz (WRC-12) !
      L'utilisation des technologies cellulaires (4G/5G) est à l'étude …
  - **Grand Public:**
    - Bandes non licenciées (ISM 2,4GHz & 5,5GHz)

Base Télécom
Normalisation

- Ex:
- STANAG 4586 : Architecture drone et charge utiles
- STANAG 7085 : Liaison de données –Structure



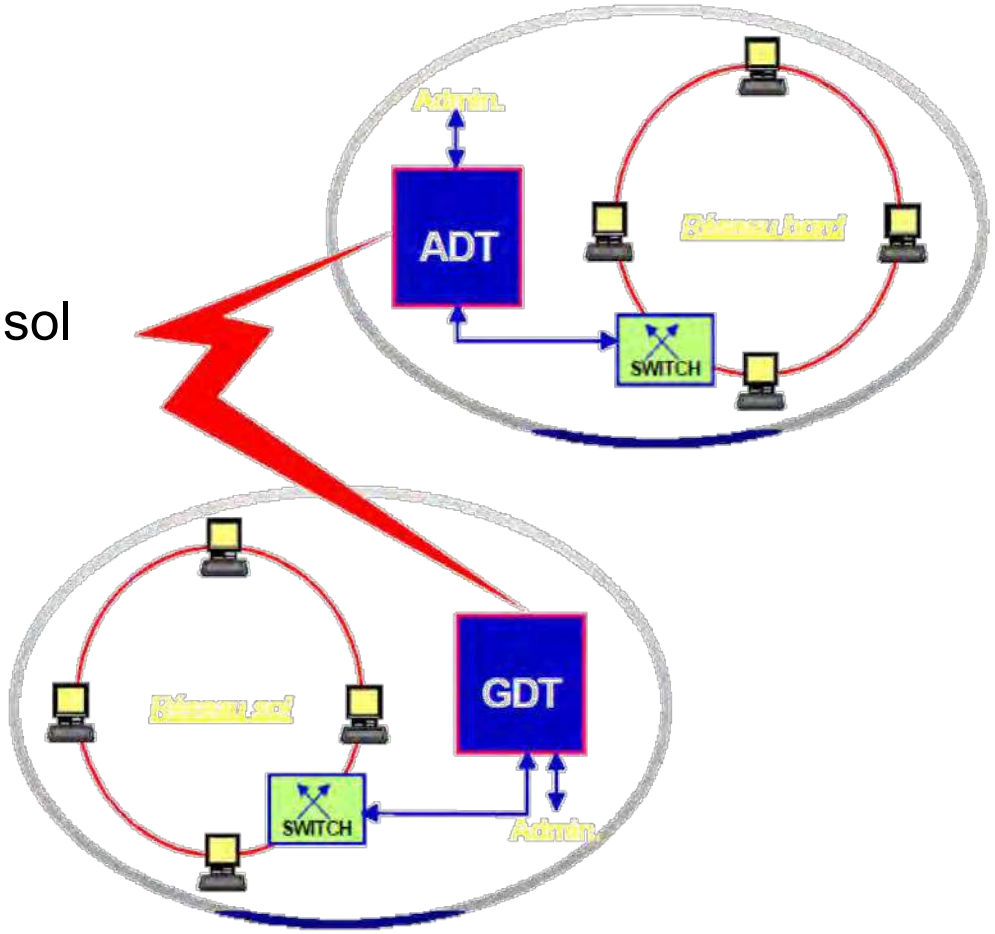
Base Télécom
Normalisation

- Le **STANAG 7085** définit la forme d'onde du canal descendant.
- Pas de convergence sur un mode unique au niveau mondial rendant difficile voire impossible l'interopérabilité.

- Plusieurs implémentations d'un mode minimal non compatibles:
  - Implémentation américaine «CDL»: OQPSK + Reed Solomon (10,7Mbps)
  - Implémentation Française: basée sur le standard DVBS (QPSK + Convolutionnel-Viterbi) (10,7Mbps)

Base Télécom
Normalisation

- Tendances:
  - Réutilisation de l'acquis ***IP*** du monde civil.
  - Interopérabilité au niveau 3 très facile.
  - Organisation en réseau des parties embarquées et au sol

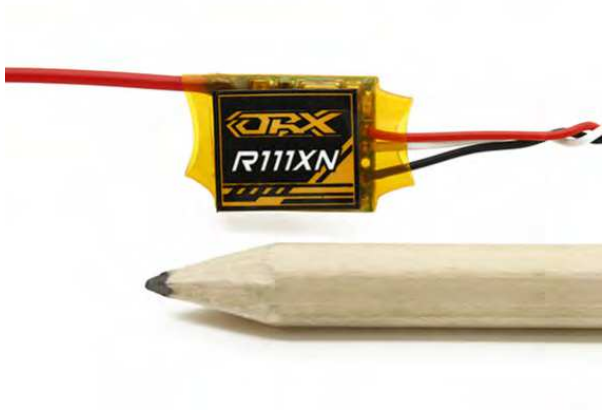


AIRBUS

Base Télécom
Modems

- Exemples:

- Drone loisir moyenne gamme



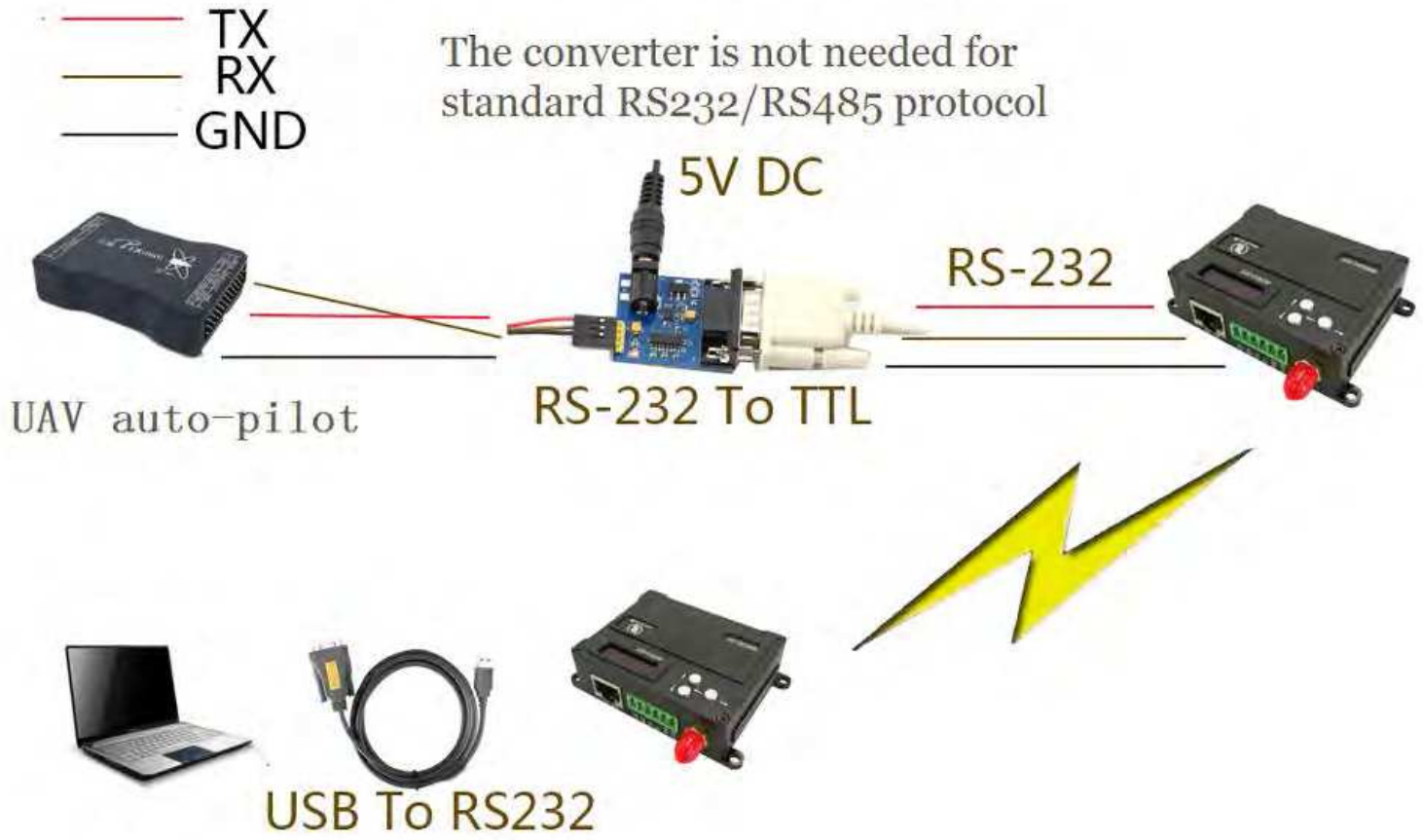
AIRBUS

Base Télécom
Modems

- Exemples:

- Drone loisir haut de gamme
- Portée <2 km

MAVLINK

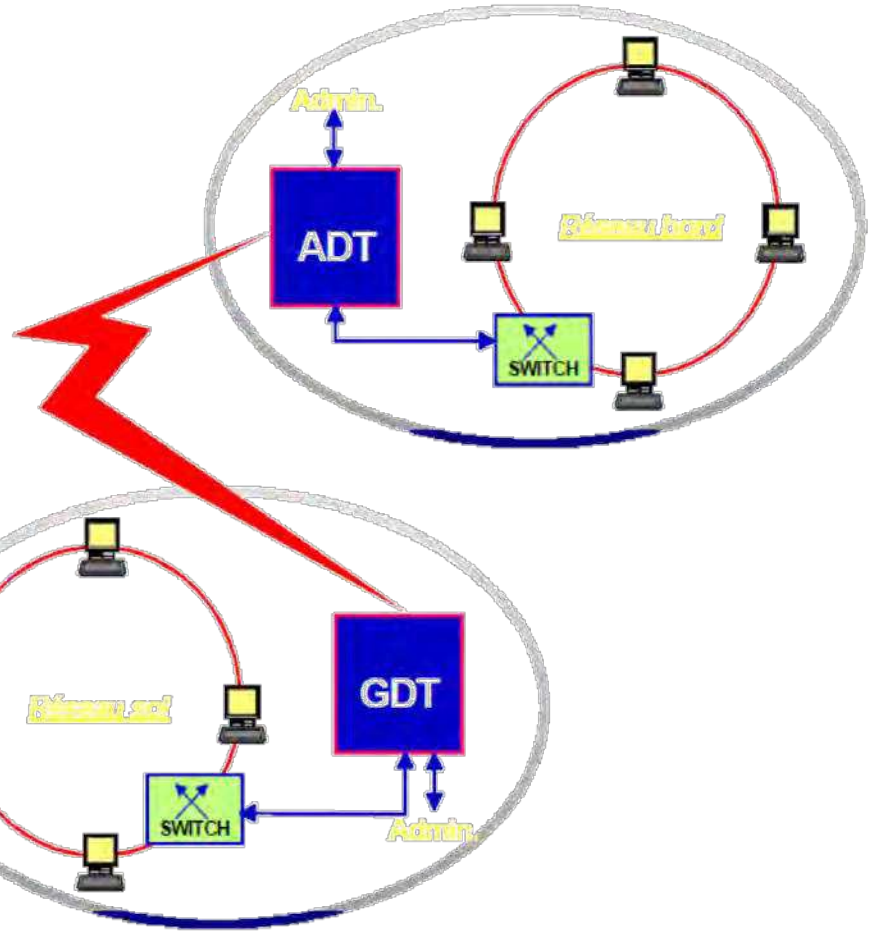


AIRBUS

Base Télécom Modems

- Exemples:

- Drone env. 25kg
- Portée 1-50km



AIRBUS

Base Télécom Modems

- Exemples:

- Drone militaires €€€

AIRBUS

Base Télécom Modems

- Exemples:

- Drone militaires €€€

General

Waveform	Mobile Networked MIMO (MN-MIMO™)
Modulation	C-OFDM; BPSK, QPSK, 16-QAM, 64-QAM
Channel Bandwidth	5, 10 & 20 MHz (1.25*, 2.5*)
Encryption	DES Standard, AES 128/256 Optional (FIPS 140-2)
Frequency Stability	1 PPM over temp -40° - +85° C
Tuning Step Size	1 KHz
Data Rates	Max 85 Mbps UDP & 70 Mbps TCP
Error Correction	1/2, 2/3, 3/4, 5/6
MIMO Diversity	2x2
MIMO Techniques	Spatial Multiplexing, Space-Time Coding, Eigen Beam Forming
No. of Spatial Streams	1-2
No. of Antennas	2
Total Power Output	10mW – 500mW (variable)

Performance

Latency	7 ms average (20MHz BW)
Sensitivity	Varies with MCS index and BW Maximum = -99 dBm (5 MHz BW, MCS 0)
Frequency Bands	Dual Band; Bands from 400MHz to 6GHz Available

Low Band		High Band	
Band (Freq. Code)	Frequency Range	Band (Freq. Code)	Frequency Range
UHF (042)	400-450	Low C Band (455)	4400-4700
ISM 900 (091)	902-928	High C Band (485)	4700-5000
L Band (137)	1350-1390	5.2GHz ISM (520)	5150-5250
Broadcast A (209)	1980-2200	5.8GHz ISM (580)	5725-5875
Broadcast B (206)	2025-2110		
Federal 'S' (225)	2200-2300		
Federal 'S' + 2.4GHz ISM (235)	2200-2500		
2.4GHz ISM (245)	2400-2500		

Environmental

	Standard Temperature	Extended Temperature
Ambient Temp.	-40° - +55° C	-40° - +65° C
IP Rating (Ingress Protection)	IP-67 (Dust / Immersion in water up to 1m) *	

*Must have all connectors mated and use IP67 or better cables/antennas

Mechanical – Chassis

In addition to the physical system package described here, Silvus offers the core board-stack for integration into an OEM product

	Standard Temperature	Extended Temperature
Dimensions	4.4" x 3.4" x 1.3"	4.4" x 3.4" x 2.0"
Weight	1.0 Pounds	1.2 Pounds
Color Options	a. Black anodized b. FED-STD-595B-34094 (Green 383)	
Mounting	4-hole mounting patterns (Through-hole)	

AIRBUS

Base Télécom Modems

- Exemples:
- Drone militaires €€€

- Débit maximal 12 Mbps utiles.
- Antennes mobiles embarquées :
  - > Hélice, Quadrifilaire
  - > Zeppelin
- Puissance 30 dBm
- Service -40° à + 85° ambiant
- Alimentation 7 - 17 VDC
- Consommation 6 watts
- Fréquences OEM : 902-928MHz/2304-2364MHz/5.0-5.8GHz
- Fréquences Standard 2405/2470 MHz

* Portée selon les antennes utilisées

Base Télécom Modems

- Exemples:

- Drone militaires €€€

- **Emetteur Récepteur IP TDD COFDM** ultra léger en boitier aluminium usiné.
- **Full Duplex** transmet et reçoit de la vidéo HD ou SD en H264 et des data.
- Configuration du menu pour opérations en temps réel avec préréglages.
- Hautes performances de la modulation COFDM et de la polarisation RHCP
- Longue portées sans pointage d'antennes (Quadrafilaires Omnidirectionnelles)
- Récepteurs Emetteurs multiples en PMPT et monitoring selon les applications.
- Fonctionne en mode non à vue en mobiles à haute vitesse de déplacement .

HYC-540 est intégré en Région Languedoc Roussillon -CEE-
Hypercable -Innoveum -74 Avenue Paul Sabatier-11100 NARBONNE
www.hypercable.fr
info@hypercable.fr

Fréquences: 2405 – 2470 MHz (Autres sur demande)
Puissance: 30 dBm – 1 watt
Seuil de sensibilité: -99 dBm
Alimentation: 7/17 VDC 6 watts
Modulation: COFDM Time Division Duplex mode
Canaux: 4 ou 8 MHz au pas de 1 MHz
Canaux: 4 et 8 MHz au pas de 1 MHz
Ethernet: 10/100 BaseT Auto-MDI/X IEEE 802.3 TCP , UDP,TCP/IP,TFTP,ARP,ICMP,DHCP,HTTP,SNMP,FTP,DNS
Encryption: AES 128 bit et AES 256 bits
Correction d'erreurs: CRC-ARQ 32 bits
Température de service: -40° +85° C
Dimensions poids: 75x51x22 mm 120 grammes
Réglages: écran de contrôle OLCD

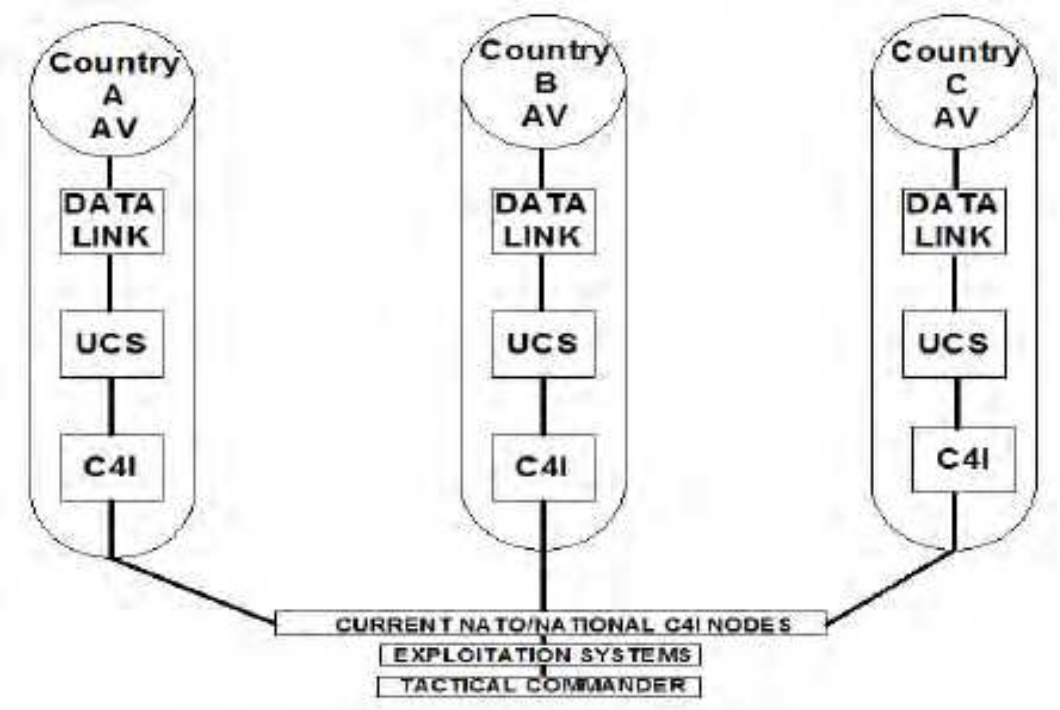
Product features:

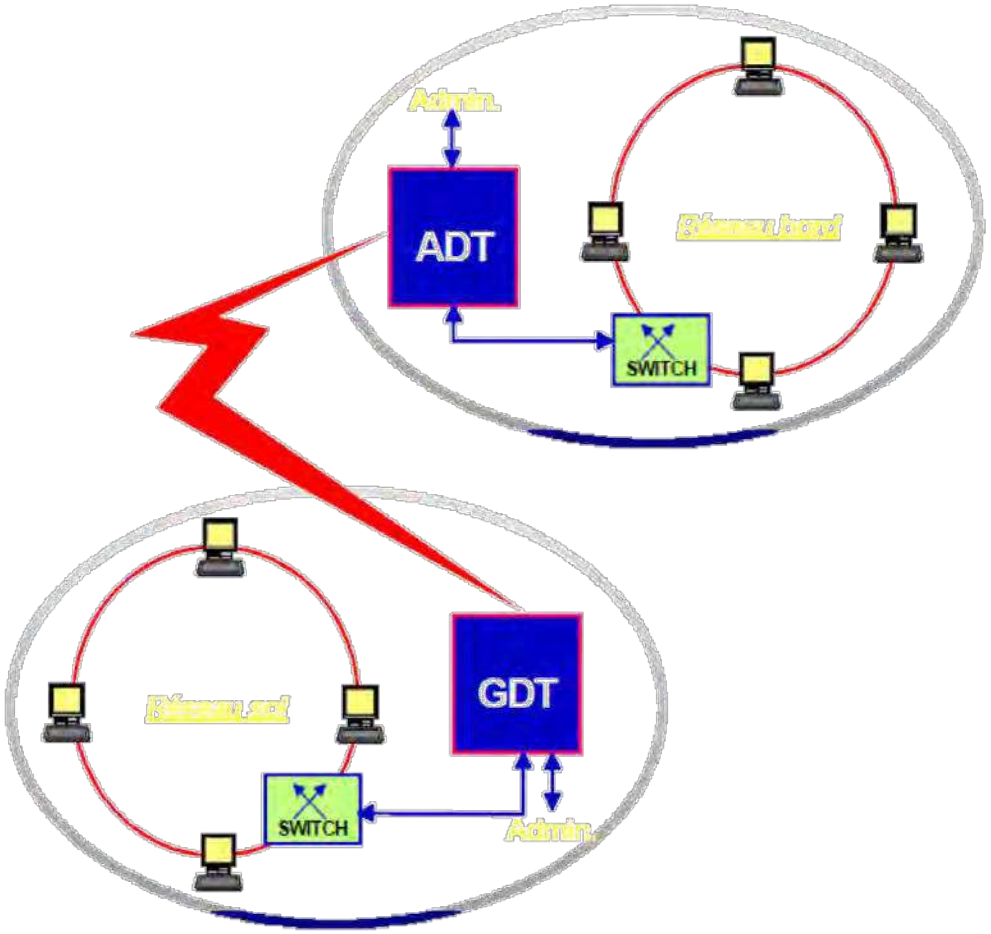
- Provide up to 12Mbps data stream, dynamic adaptive rate allocation technology
- Support transparent PMPT network technology
- Support for non line of sight (NLOS) ,high-speed mobile transmission
- Provide standard RS-232&RS-485 + RJ45
- Support high standard industrial applications
- Small volume, light weight, easy to carry, fin type aluminum chassis
- High definition OLED panel digital display, simple interface and easy to operation

Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

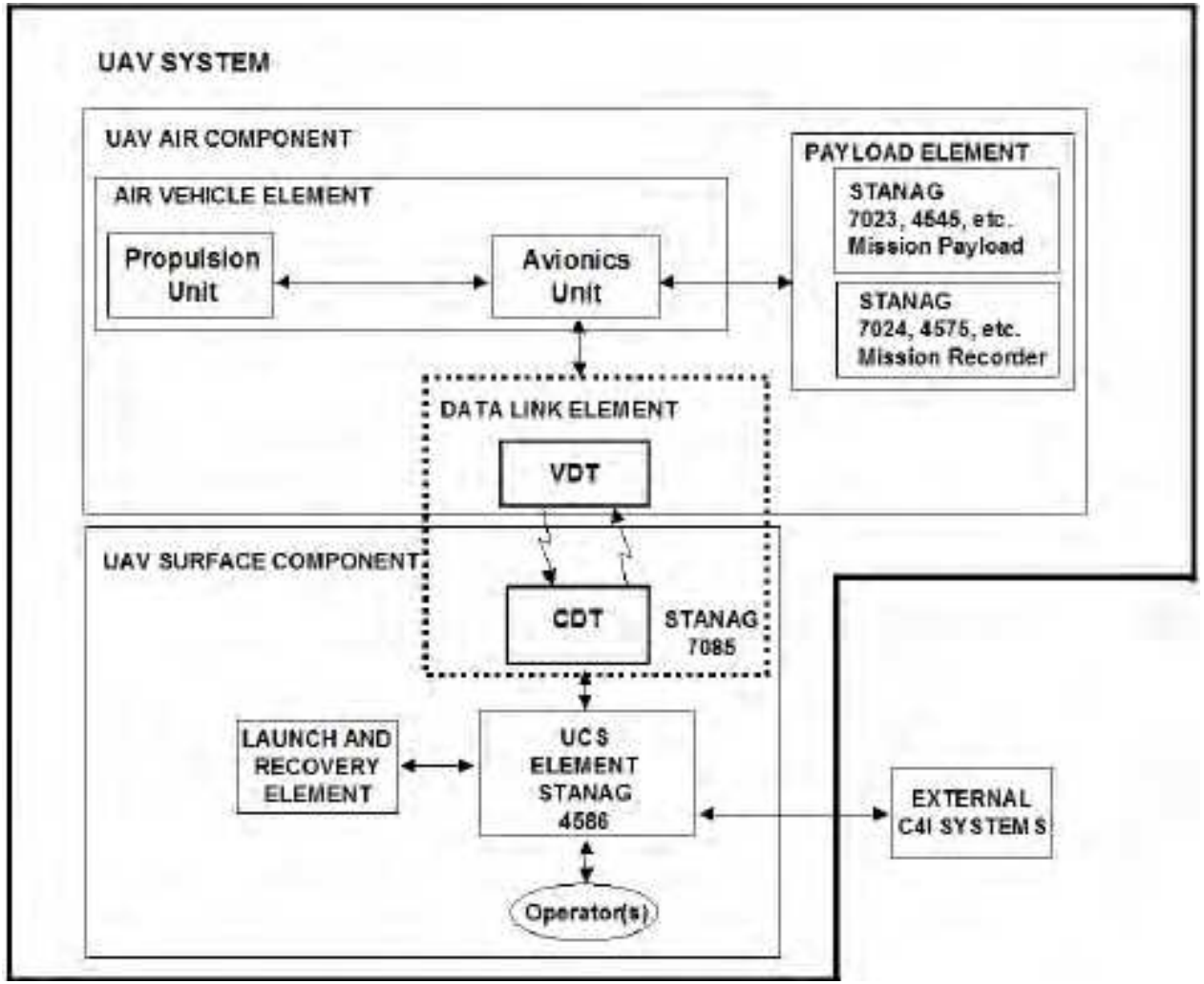
Architecture

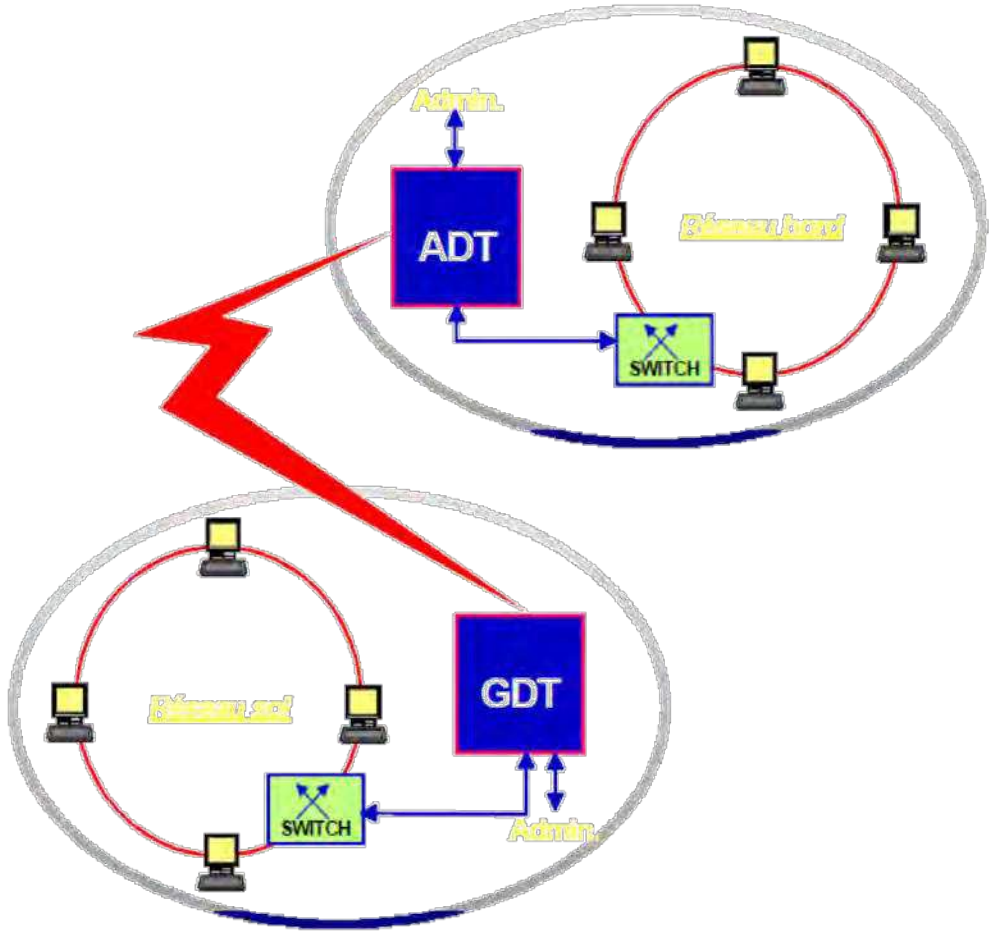




AIRBUS

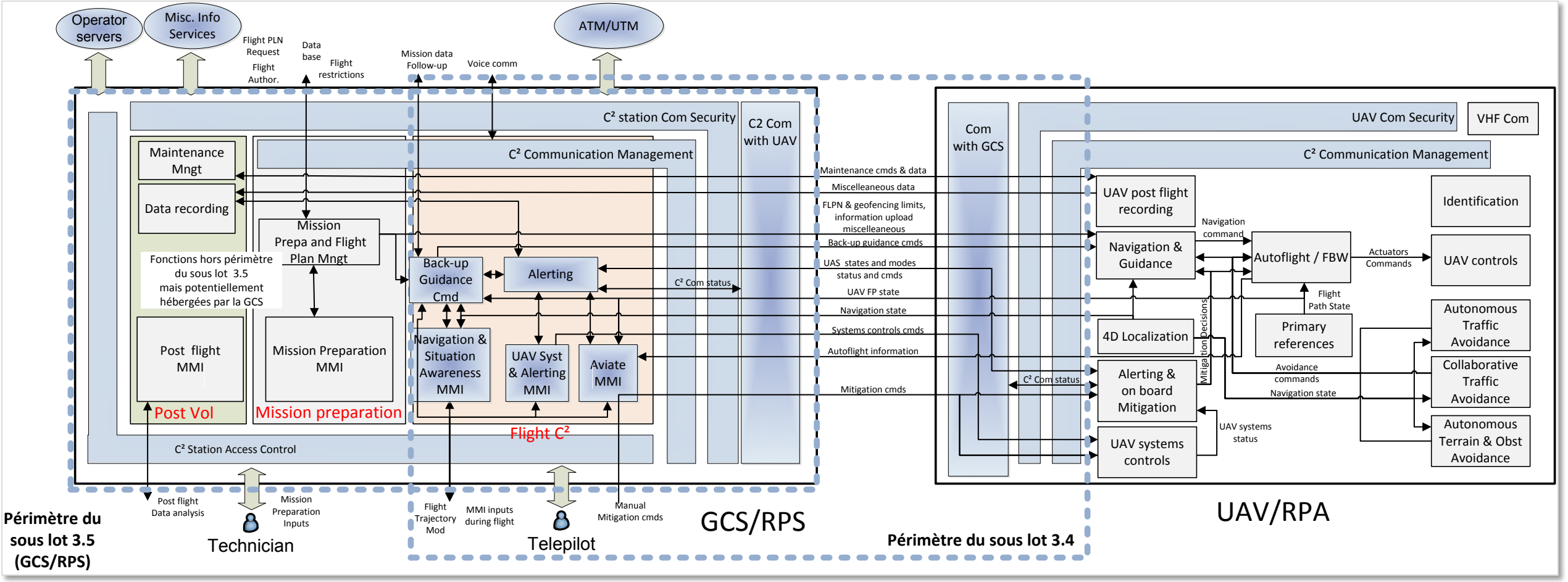
Architecture





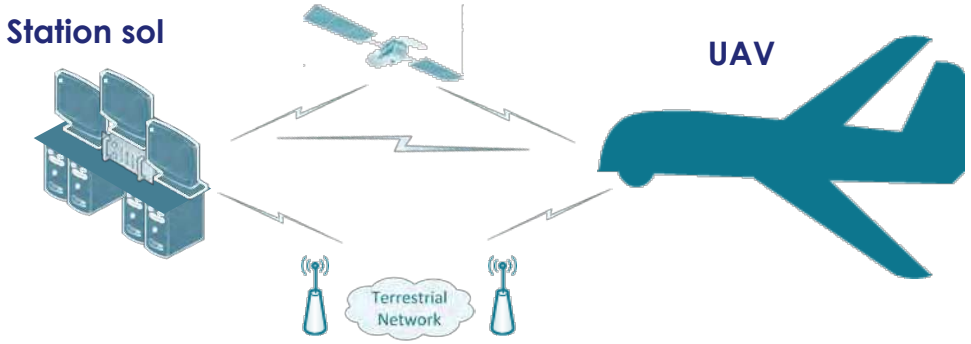
AIRBUS

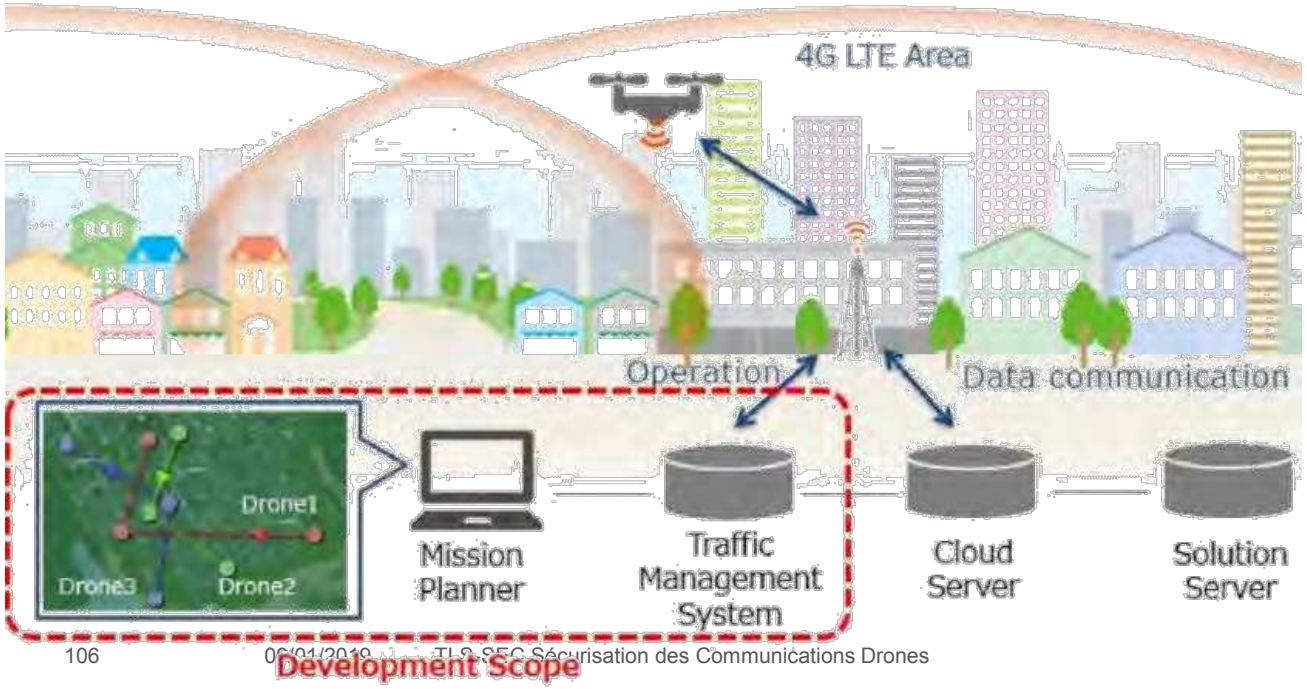
Architecture

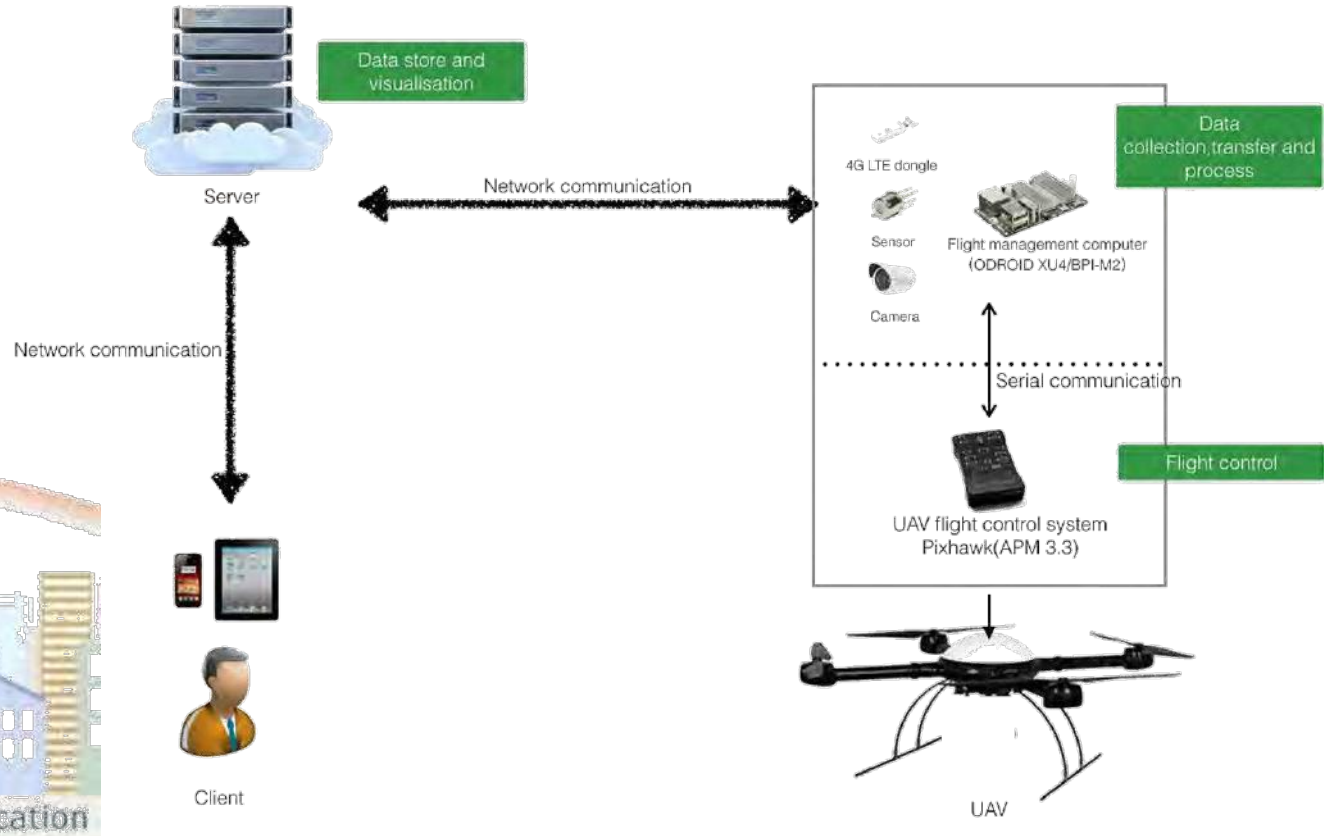


AIRBUS

Architecture







AIRBUS

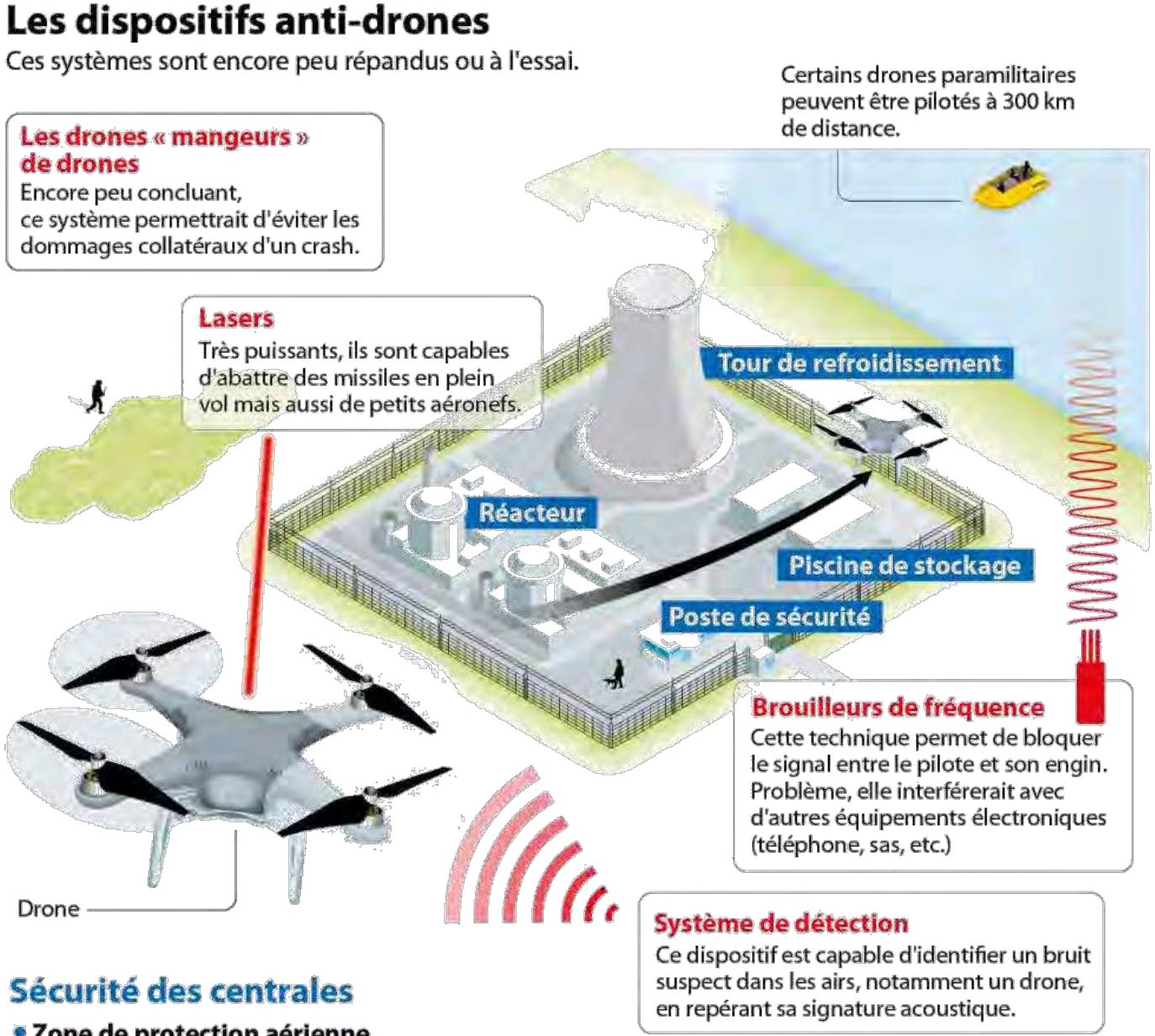
Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

Menaces

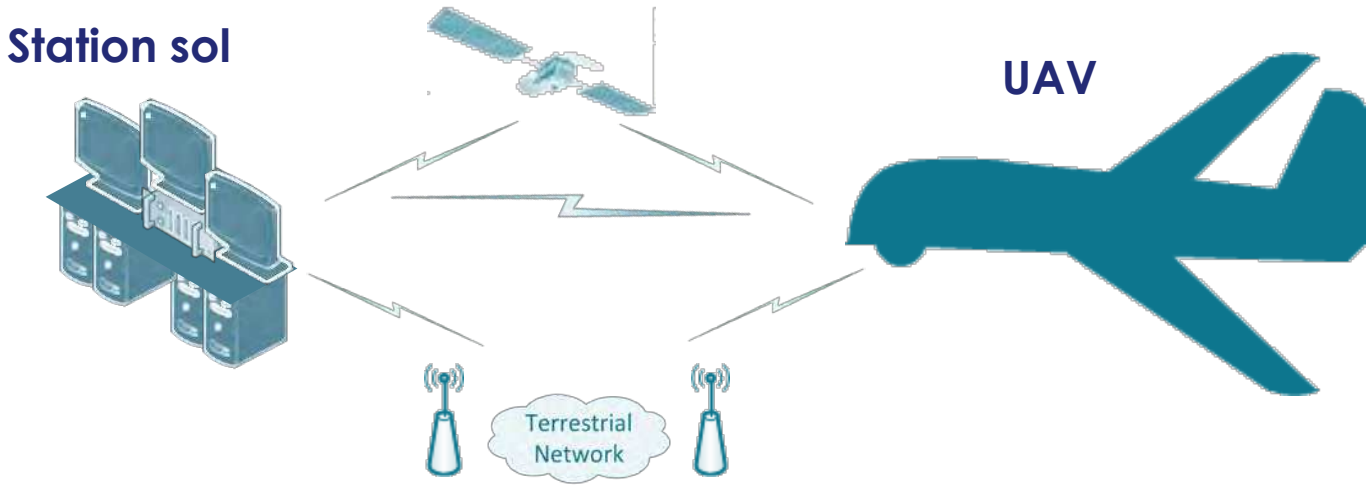
- Menaces cyber « classiques »: liaisons IP

- Menaces « radio »
  - Lutte anti-drone civile
  - Lutte anti-drone militaire



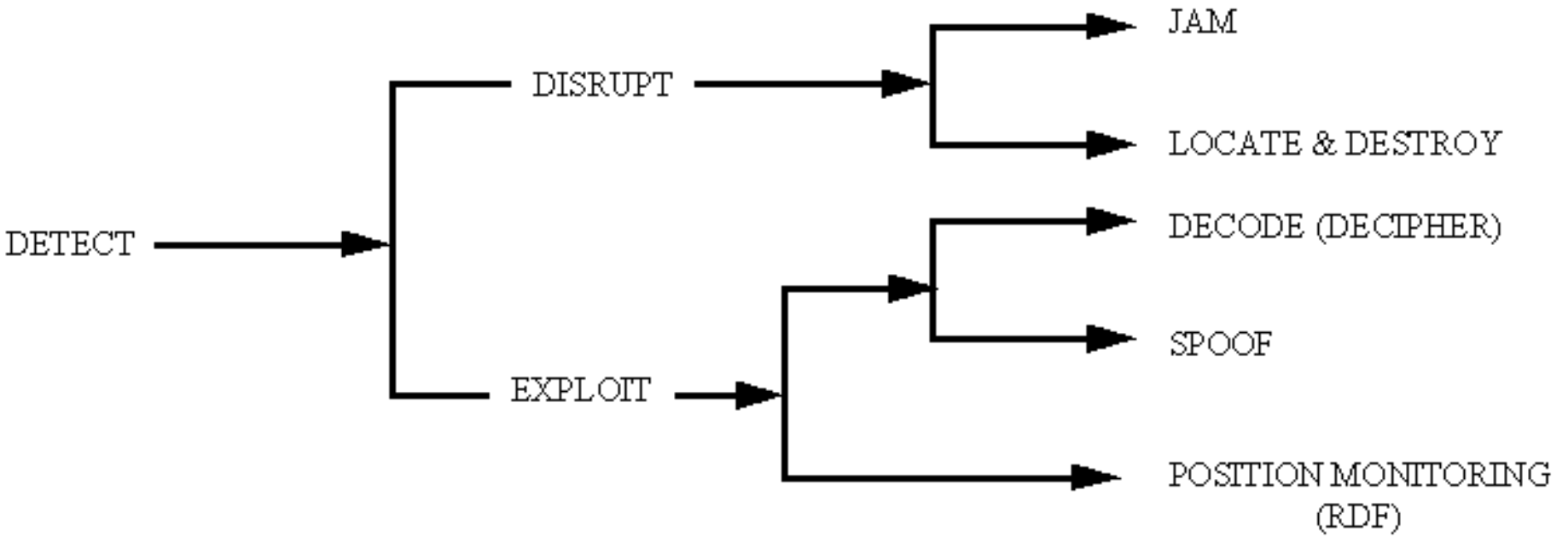
Menaces

- Menaces cyber « classiques »: liaisons IP
  - Attaques sur le lien sol de contrôle via entrée IP
    - Encore plus évident si utilisation d'un réseau commercial 3G/4G/5G



Menaces

- Menaces « radio »
- Stratégies



Electronic Warfare Overview for Military Systems (c) 1996 Steve F. Russell

Menaces

- Menaces « radio »

- Au niveau du drone émissions radio très faibles:
  - Antenne(s) petite(s) donc faible gain
  - Puissance électrique limitée à bord, donc RF
    - Puissance RF en fonction de leur domaine de vol / évolution
      - Loin (>10km) pour les gros drones militaires
      - Moyenne portée pour les drones de taille moyenne
      - Courte portée pour les drones civil et de loisir

→ Détection visuelle et radio peu aisée

Menaces

- Menaces « radio »

- Tout comme les stations sol de pilotage, il faut une antenne à fort gain et donc directive pour repérer le signal TC du drone

  → scan du ciel en permanence

  - Aide des radars pour les drones militaires

- Mesures de discrétion pour les gros drones militaires rendant presque impossible leur détection

Menaces

- Menaces « radio »
  - Radars pour le moment limités pour les drones 25kg et moins: env. 1km max

AIRBUS

Menaces

- Menaces « radio »

- Brouillage possible via connaissance à priori de la position du drone
  - Plus la position sera connue avec précision plus on pourra concentrer de la puissance de brouillage
  - Présence de beaucoup de puissance RF sur brouilleur militaire

AIRBUS

Menaces

- Menaces « radio »

- Brouillage possible via connaissance à priori de la position du drone
  - Ciblage fusil sniper pour les petits drones

AIRBUS

Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

Sécurisation

- Sécurisation réseau

- Sécurisation radio

Sécurisation

- Sécurisation réseau : moyens classiques
  - Les machines informatiques destines à héberger les applications de la station sol doivent être durcies afin de réduire la surface d'attaque de ces serveurs. Le durcissement sera réalisé en suivant les guides applicables aux éléments concernés, a minima :
    - Couches protocolaires réseau
    - Système d'exploitation
    - Logiciels mutualisés (gestionnaires de bases de données, services de messagerie, serveurs d'application…)
  - L'ouverture de session sur la station sol doit inclure l'identification et l'authentification des utilisateurs
  - Les droits d'accès aux ressources de la station sol doivent être définis pour chaque groupe d'utilisateurs et contrôlés. Notamment il convient de distinguer les rôles de :
    - Télépilote, en charge de la conduite du drone
    - Technicien, en charge du maintien en condition opérationnelle du système de drone, segment bord et sol.
    - Administrateur, en charge du maintien en condition opérationnelle de la plateforme informatique de la station sol.

Sécurisation

- Sécurisation réseau : moyens classiques
  - Les interfaces réseau de la station sol doivent être protégées contre l'intrusion et les connexions non autorisées
  - Seules les machines authentifiées par des mécanismes cryptographiques reconnus sont autorisées à ouvrir une connexion avec la station sol
  - La station sol doit élaborer et conserver de manière sécurisée un historique des évènement opérationnels et de sécurité
  - La station sol doit faciliter la validation des données entrant dans le dossier de vol, en provenance de fournisseurs de service non approuvés (untrusted).
  - La station accepte uniquement le transfert de données de/vers un support physique préalablement authentifié.

Sécurisation

- Sécurisation radio
  - Spécifications de la liaison de donnée:

- Débit/Portée
- Taux d'erreur de bit
- Taux d'effacement messages
- Temps de latence
- Temps d'acquisition
- Efficacité spectrale
- …

→

- Seuils de fonctionnement
- Seuils d'acquisition
- Marges d'antibrouillage
- ...

↓

Disponibilité géographique & temporelle

Raisonnement principalement pour un usage militaire

Sécurisation

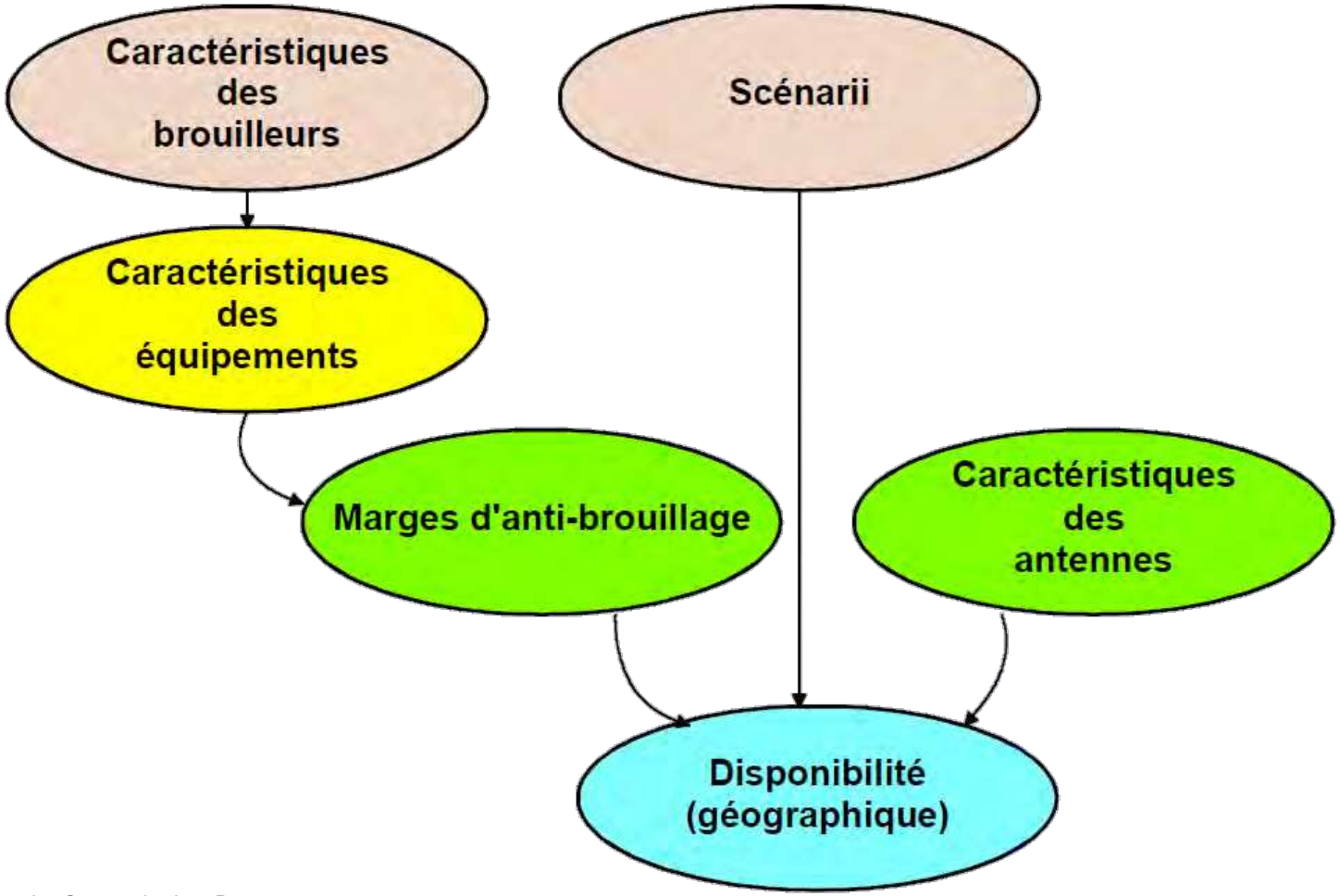
- Sécurisation radio
  - Transec – Transmission Security
    - Partie radio pure
  - Comsec – Communication Security
    - Partie radio + protocolaire + cryptographique + réseau

Sécurisation

- **Exemples:**
- Performances de transmission (temps clair)
  - TC, TM: Disponibilité temporelle > 99 %
  - Données: Disponibilité temporelle > 90 %
  - Remarque: Les disponibilités TM et Données étant différentes, le multiplexage temporel est à éviter. Un multiplexage par codes d'étalement par exemple est préférable
- Performances de transmission (brouillage)
  - TC, TM: Disponibilité géographique > 90 %
  - Données: Disponibilité géographique > 80 %
- Performances de localisation
  - Distance: < 20 m
  - Angle : < 5 mrad

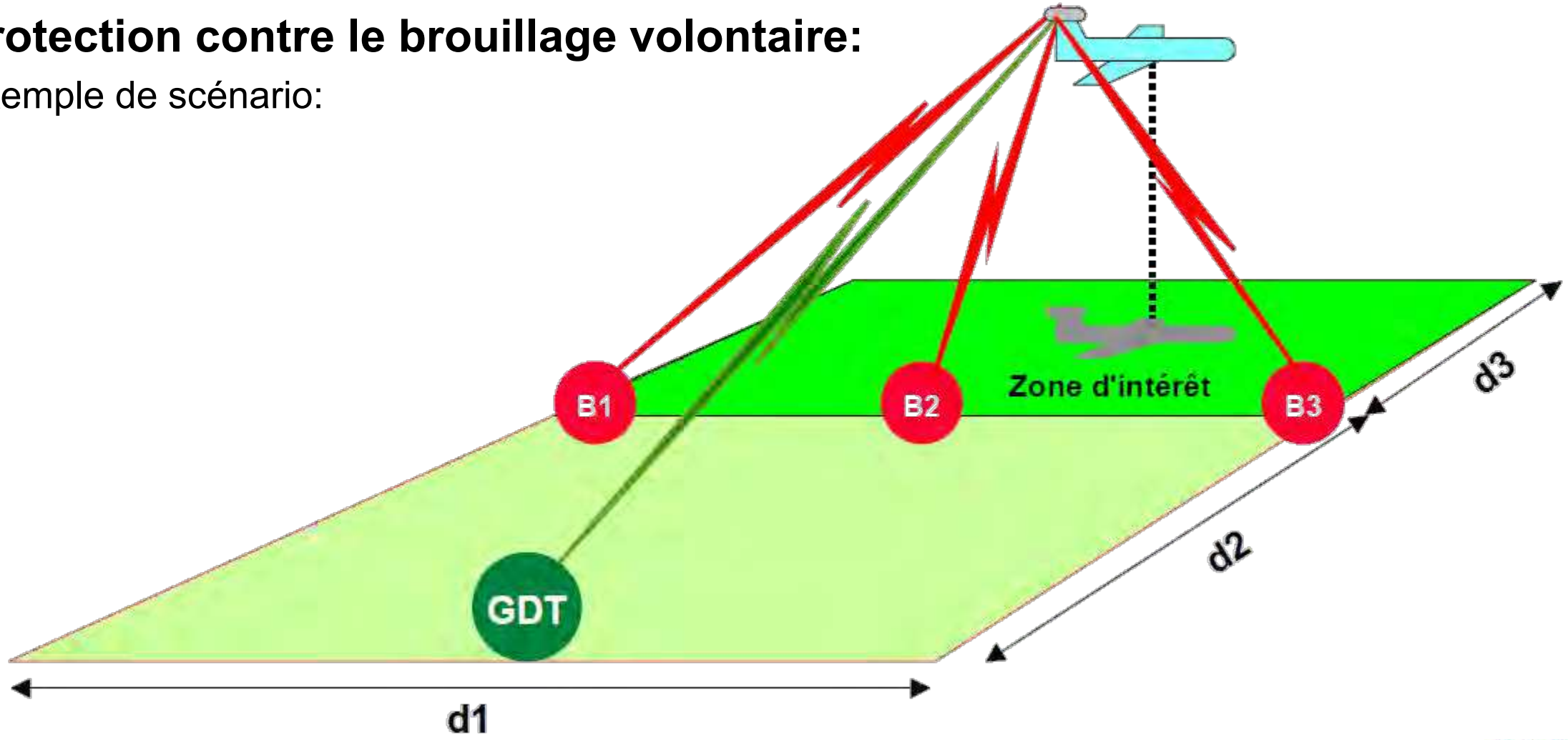
Sécurisation

- **Protection contre le brouillage volontaire:**
- Méthode d'analyse:



Sécurisation

- **Protection contre le brouillage volontaire:**
- Exemple de scénario:



AIRBUS

Sécurisation

- **Protection contre le brouillage volontaire:**
- Différentes classes de brouilleurs potentiels
- La conception de la liaison doit anticiper la stratégie adaptative du brouilleur. La caractéristique stable étant la puissance moyenne du brouilleur. Celui-ci est en effet capable de:
  - Adapter sa bande de fréquence à la liaison à brouiller
  - Adapter son facteur de forme et sa fréquence de répétition
  - Eventuellement déterminer en temps réel le canal fréquentiel utilisé par la liaison
- Le niveau de résistance de la liaison est déterminé par l'AJM (Anti Jamming Margin – Puissance brouilleur / Puissance liaison) mesuré quand le brouilleur s'est adapté pour une efficacité maximale

Sécurisation

- **Protection contre le brouillage volontaire:**

- Niveaux de protection (classification non normalisée)
  - Niveau 0 : Comportement non prédictible en présence de brouillage
  - Niveau 1 : Comportement prédictible
  - Niveau 2 : Comportement prédictible avec prise en compte en conception de moyens de protection

Sécurisation

- **Protection contre le brouillage volontaire:**

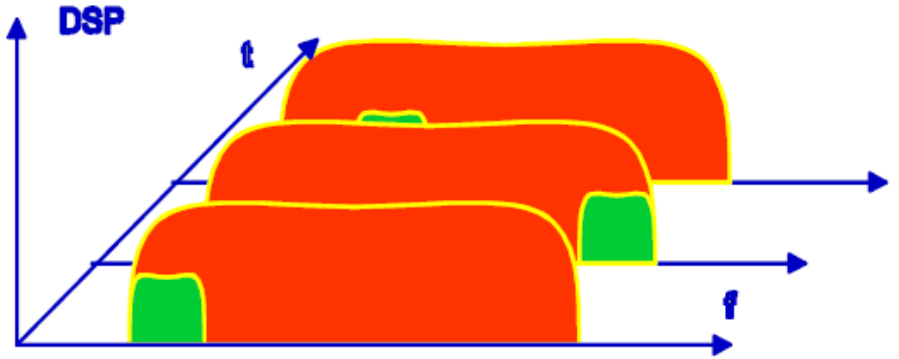
- La performance système se chiffre en **pourcentage de disponibilité géographique** sur une zone d'intérêt. Elle prend en compte:
  - Un scénario géographique: zone d'intérêt, disposition des brouilleurs.
  - Les caractéristiques des brouilleurs:
    - Puissance
    - Forme d'onde
    - Capacités d'adaptation

- Les performances non chiffrés se traduisent par une mention LPI / LPD
  - **LPD**: Low Probability of Detection: émissions radio peu détectables
  - **LPI**: Low Probability of Interception: SI détection, quasi impossibilité à retrouver l'information

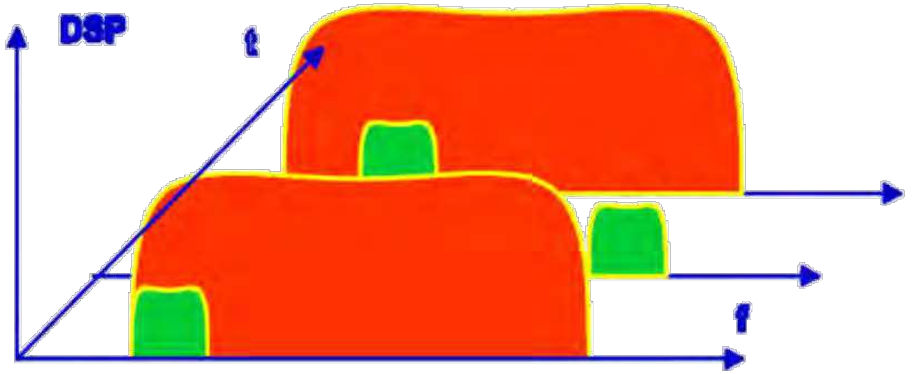
Sécurisation

- **Protection contre le brouillage volontaire:**

- Classes de brouilleurs:



Brouilleur Continu Adaptatif



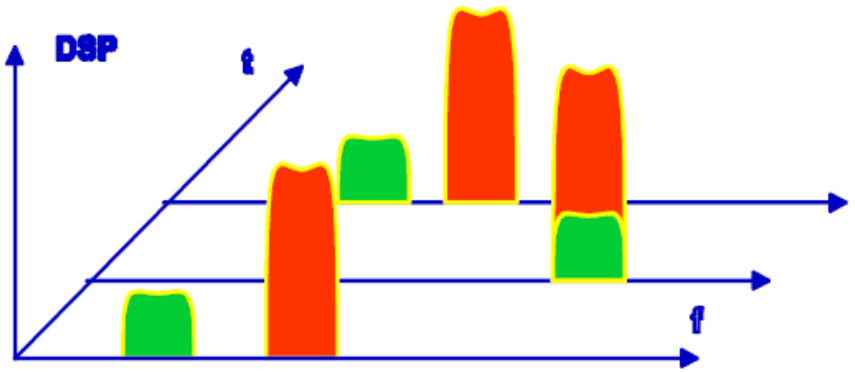
Brouilleur Impulsionnel Adaptatif

AIRBUS

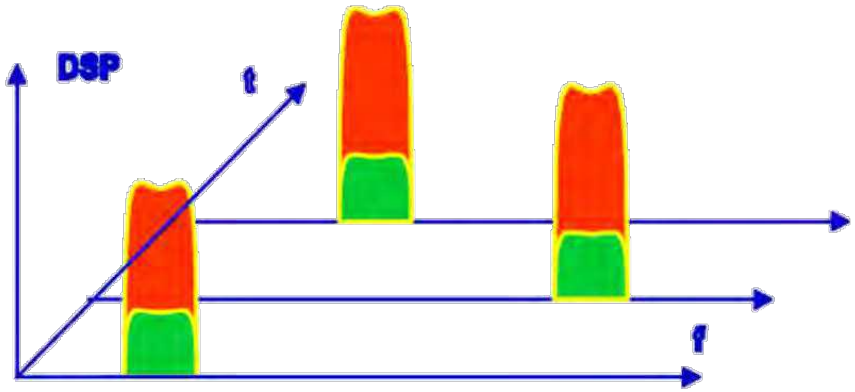
Sécurisation

- **Protection contre le brouillage volontaire:**

- Classes de brouilleurs:



Brouilleur Bande Etroite Agile



Brouilleur Intelligent

AIRBUS

Sécurisation

- **Protection contre le brouillage volontaire:**

- L'amélioration apportée par un choix judicieux du couple *modulation / codage* étant limité par l'asymptote de SHANNON, la seule solution pertinente est l'augmentation artificielle de la bande utilisée de façon à obliger le brouilleur à disperser son énergie et donc à réduire le bruit N_0.
  Les techniques usuelles sont:
  - **FHSS** (sauts de fréquence aléatoires). Nécessite un codage de canal spécifique contre les effacements
  - **DSSS** (étalement par séquence directe). S'accommode d'un codage de canal optimisé pour le temps clair
  - Combinaison des deux
  - **Bursts**: transmissions « flash » impromptues
  - **Directivité**

Sécurisation

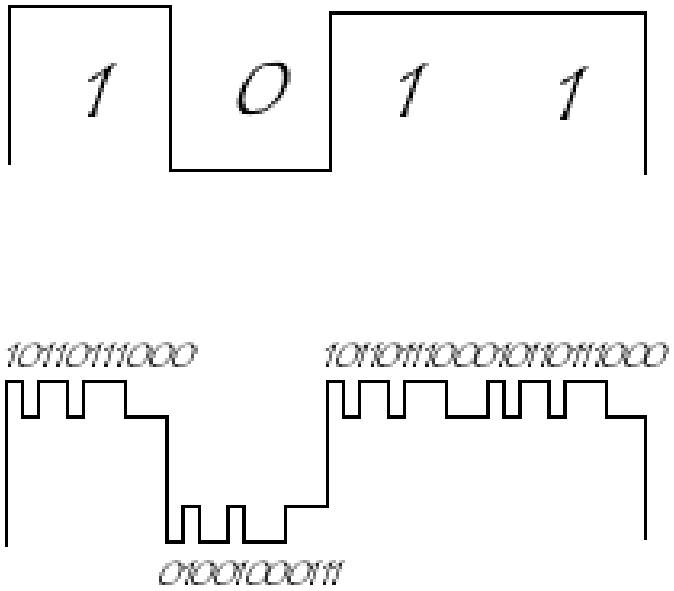
- **Protection contre le brouillage volontaire:**
  - **FHSS – Frequency Hopping Spread Spectrum** (sauts de fréquence aléatoires). Nécessite un codage de canal spécifique contre les effacements

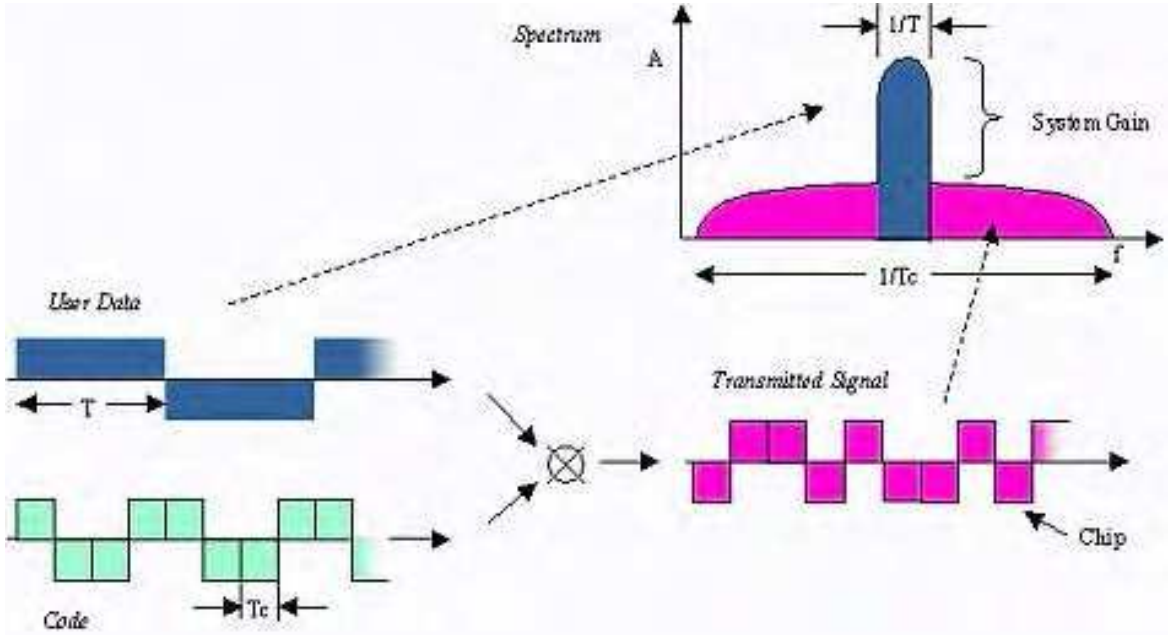
Sécurisation

- **Protection contre le brouillage volontaire:**

Utilisé aussi pour de l'accès multiple = CDMA comme pour la 3G

  - **DSSS – Direct Sequence Spread Spectrum** (étalement par séquence directe).
    S'accommode d'un codage de canal optimisé pour le temps clair

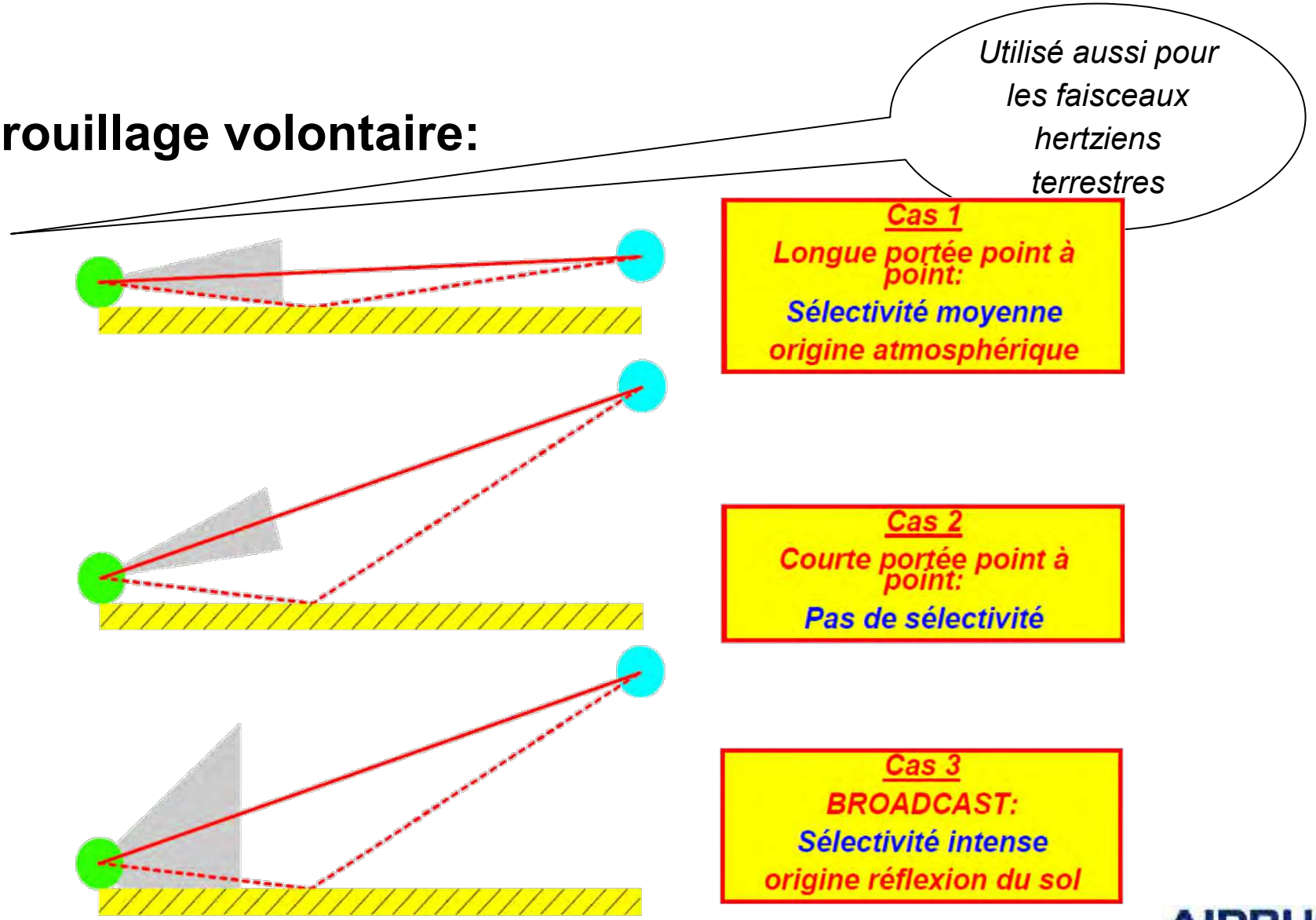




AIRBUS

Sécurisation

- **Protection contre le brouillage volontaire:**
  - **Directivité** (antenne).



AIRBUS

Sécurisation

- **Protection contre le brouillage volontaire:**
  - **Synthèse et protections adaptées:**

TYPE DE BROUILLEUR	PIRE MOYENNE	PIRE CRETE	Type de Protection adaptée			
			Agilité de fréquence	Séquence directe	Codage de canal	Discrétion
CW Adaptatif	** kW	** kW	●●●	●●●	●	●
Pulsé Adaptatif	** kW	*** kW	●●●	●●●	●●●	●
Bande étroite à saut	** kW	** kW	●●	●●●	●●●	●
Intelligent	** kW	** kW	●	●●●	●	●●●

Sommaire

- Introduction
- Missions & technologies
  - Drones civils
  - Drones militaires
- Eléments de Base en Télécom / technique
  - Propagation
  - Chaîne Télécom
  - Fréquences
  - Normalisation
  - Modems
- Architecture
- Menaces
- Sécurisation / Protection contre le brouillage
- Conclusion / discussions

Conclusion

- **Drones militaires:**
  - Moyens €€€ pour de gros brouilleurs
  - Moyens pour du matériel adapté anti-brouillage
  - Moyens pour la protection des réseaux militaires

- **Drones civils:**
  - Liens radio plus simples :
    - vulnérable à du brouillage
    - Vulnérable à du hacking de protocole
  - Hacking possible de la commande:
    - Réseau commerciaux 3G/4G/5G
    - smartphone

Thank you

AIRBUS