



**Risks and opportunities of global IP aviation communications: towards multi-domain security governance**

Vulnerabilities and Global  
Security of the CNS/ATM systems  
March 27, 2019

Introduction

Aeronautical networks before and after IP

Security domains in aeronautical networks

Security governance

Conclusions

Systems engineering and research for EU and US aviation  
CNS standardisation and regulatory support  
Adoption of IT technology for new concepts across stakeholders

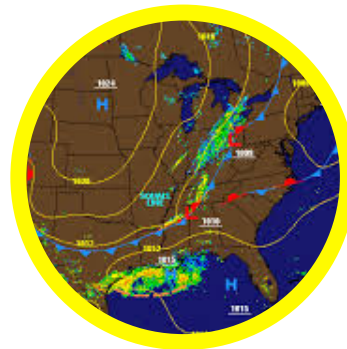
ANSPs



Airports/airlines



CSPs



Passengers



New entrants



“There are only two types of companies: those that have been hacked and those that will be”

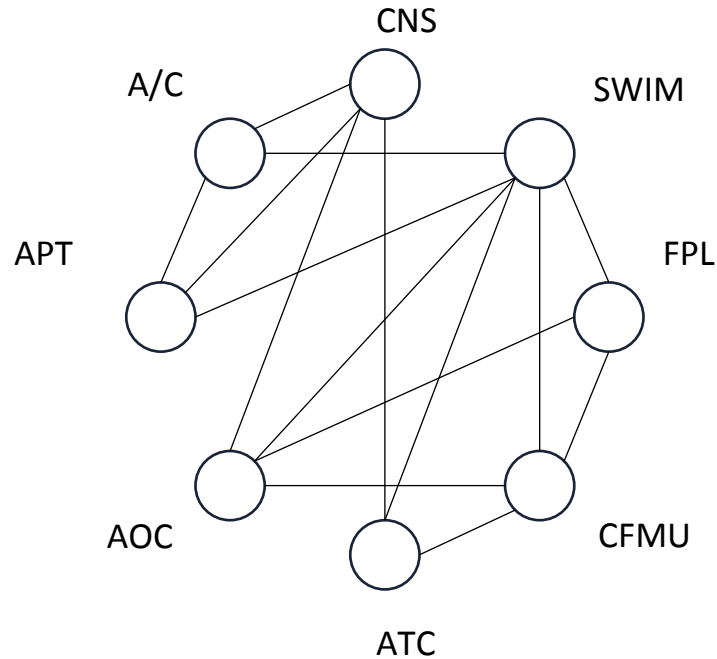
- Robert Mueller, FBI Director

“As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace”

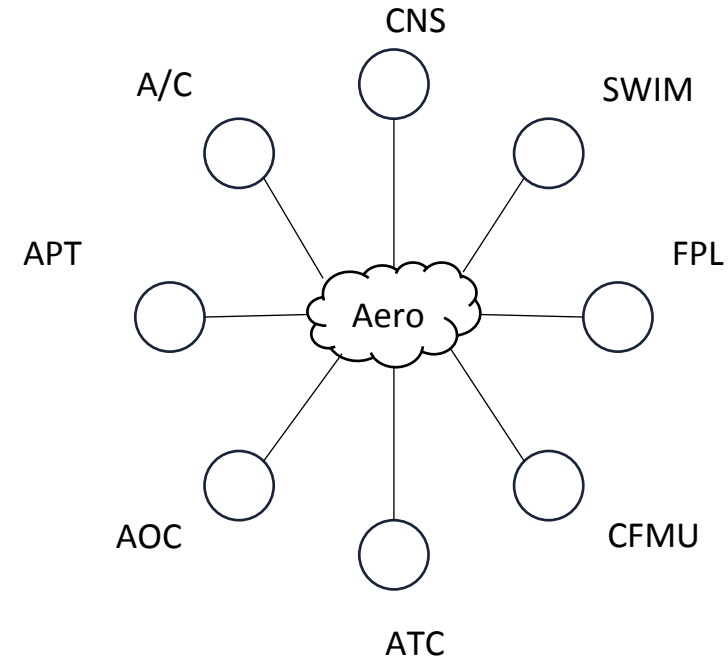
- Newton Lee, Springer science editor

“Protect your network as you protect your house: have few doors, keep your key secure, and especially don't have anything worth robbing”

- This one is mine



**BEFORE**



**AFTER**

**If the aeronautical network runs like the Internet, and has at least one entry point to the Internet, then IT IS part of the Internet**

At best, it is an enterprise network within the Internet

How to protect it?



**IP means that once you are in, you can virtually reach anywhere**

No more “security by obscurity”

**Increasing volumes of data (IoT, etc) which, isolated, are harmless**

Correlations make it dangerous

**Each stakeholder has different cybersecurity objectives**

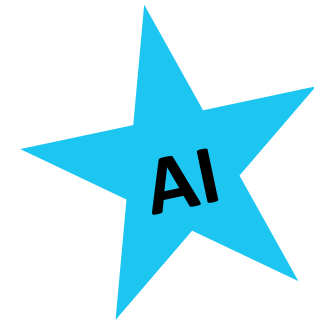
Different security assets

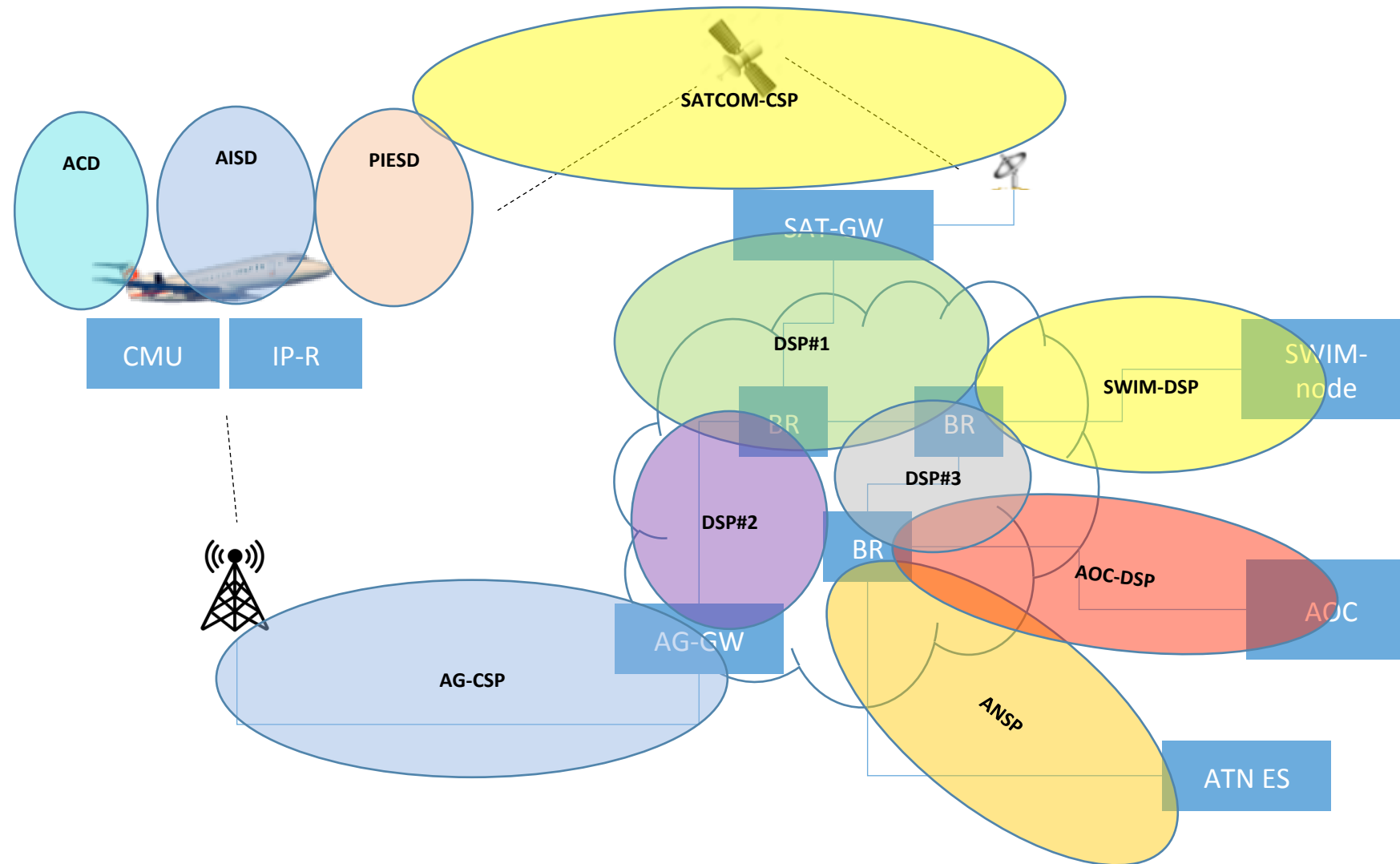
Different security vs safety tradeoff

Different CIA objectives

**Cybersecurity is much more effective to be built by design**

Minimise software updates and protocol upgrades





### Moving to data security domains is a common approach

- ICAO WG-I defines IP domains
- INNOVA defines members-only information realms
- ATN/IPS defines administrative domains and autonomous systems
- SWIM defines information domains

### Pros

- Split security assets and prevent cascade propagation
- Avoid single points of failure
- Flexibility to create overlapping domains (backup)
- Allows risk assessment methods and certification policy per application
- Scalable resilience and recovery
- Accommodation of legacy and new systems

### Con

- **Requires a clear security governance framework**



**Attributes of a security  
governance framework**

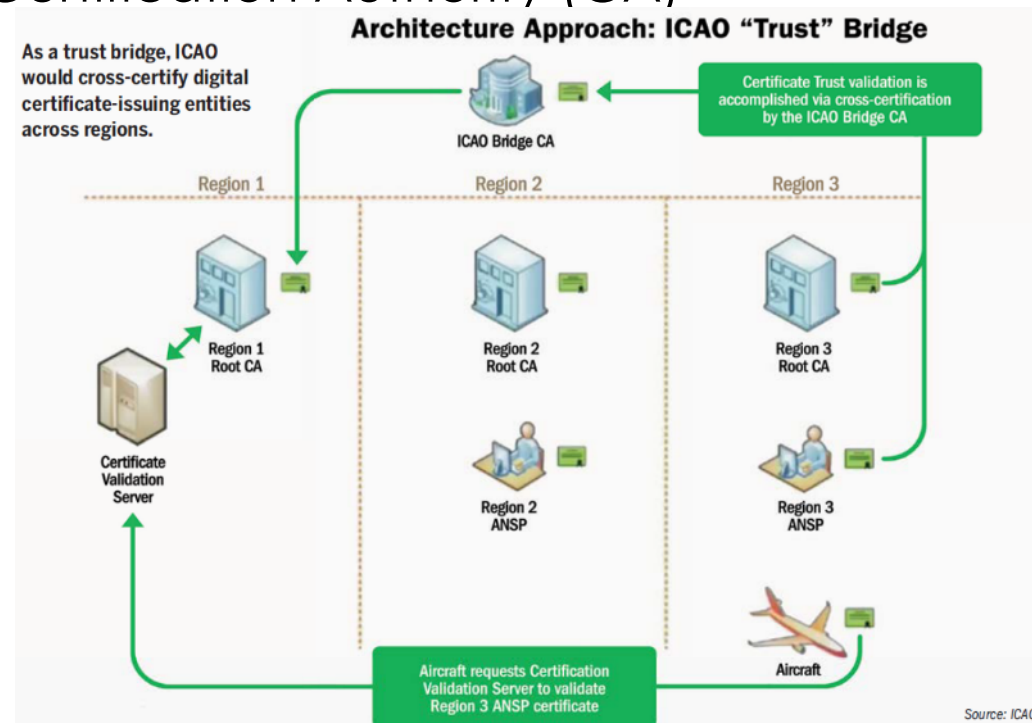
Security objectives

Trust framework

Data ownership and  
accountabilityMaintain previous  
states - recoveryInter-domain  
interface descriptionSharing of forensics  
dataIdentity  
managementCross-domain  
verification

## Some absolute security policies are needed (ICAO WG-I)

- Common time reference
- Global namespaces
- IPv6 address blocks
- Bridge PKI Certification Authority (CA)



### The importance of post-attack analysis:

- Artificial Intelligence detection, mitigation and recovery
- Enables proactive cybersecurity protection and immediate cyber center response (e.g. EATM-CERT, SITA CCTC)
- Together with blockchain, make cyber attacks not worth it!

### But:

- Needs very large amounts of data for pattern recognition and learning
- Fear of exposing data (confidentiality / reputation)
- **Critical aspect to define in security governance**

**IP aeronautical networks will follow a multi-domain architecture model**

**Holistic security risk assessments and methodologies will need to coordinate security policies in a distributed/federated manner**

**A security governance framework will help define the responsibilities of each organization within their domain and in relation to others**

**Some aspects will need to be based on absolute truths (identity management)**

**Post-attack data sharing is essential to enable the proactive cybersecurity of the future**



# Aviation of the Future

Web URL:  
[www.skymantics.com](http://www.skymantics.com)

E-mail:  
[info@skymantics.com](mailto:info@skymantics.com)