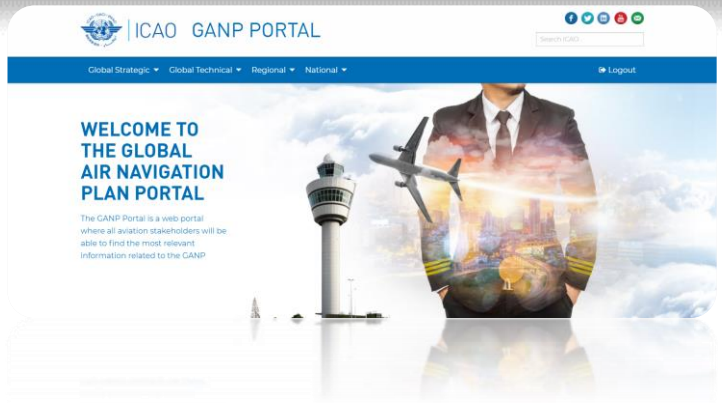
ICAO UNITING AVIATION

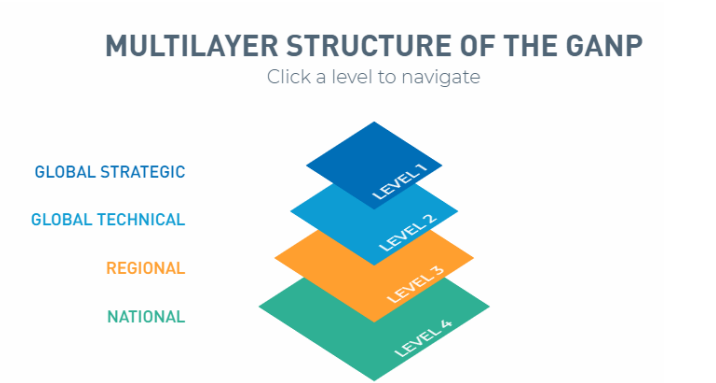
INTERNATIONAL AVIATION TRUST FRAMEWORK (IATF)

Bangkok
June 2021

Flight Plan

- Introduction
- What is the IATF?
- Digital Identity
- Network
- Conclusion





- **Information: Key for evolution**
  - Global information utilization, management and interchange
  - Aviation is moving towards the notion of full connectivity
- **Technical level**:
  - More automation
  - Digitalization of the air navigation system based on a service oriented architecture
  - Performance-driven towards a more cos-effective system
- **Places a premium on:**
  - The performance of data and information
  - Information security

https://www4.icao.int/ganpportal/

A converging strategy

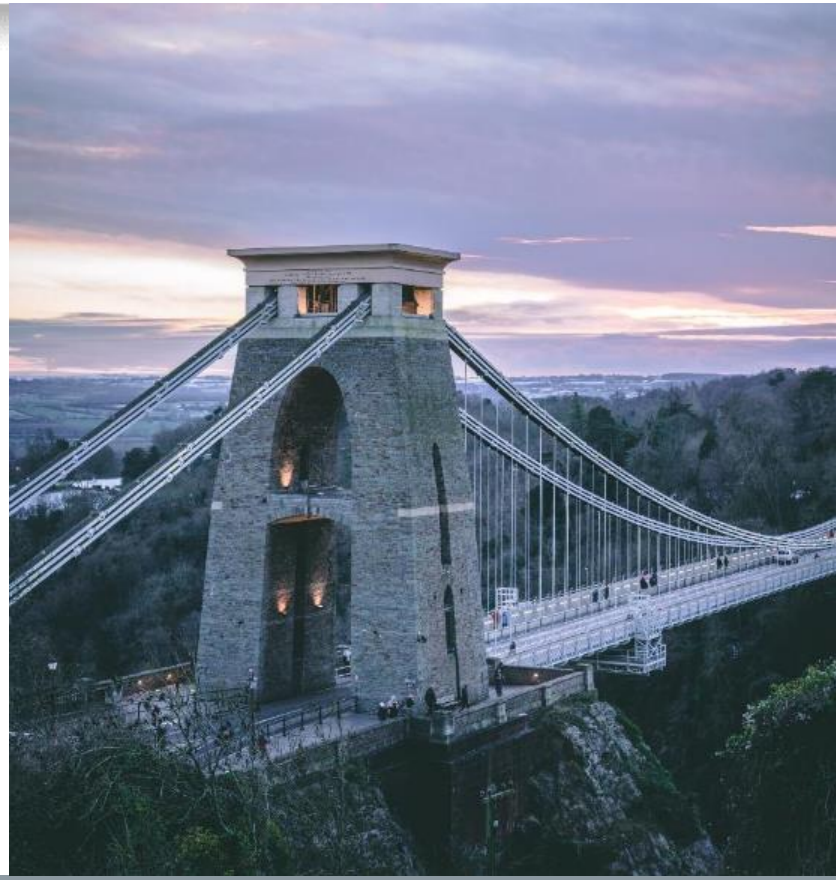
- Interoperability requires global coordination and cooperation
- Identify common needs that can unite all aviation ecosystem stakeholders
- Develop common solutions that build on existing foundations
- Agree on a common destination – where there is still one interoperable sky

What is the IATF?

- A framework to reduce the cyber-attack surface and enable reliable and trusted exchange of information for aviation using the Internet infrastructure.

Trust Framework – A Common Solution

- Foundation - International Law
  - Chicago Convention, Beijing Convention (Article 21), Annexes, etc…
- Trusted Digital Identity
  - Anchored in proven regulatory processes
- Trust Bridge
  - Allows identities to be recognized across boundaries



Trust framework

- The foundational principle of the global aviation system that connects us today
- A core function of ICAO since 1944
- An evolution of this framework now seems essential
  - Based on common standards
  - Anchored in State sovereignty
  - Facilitating global recognition of digital identities
  - Applied consistently across the aviation ecosystem

Credibility Flows from the Regulator

- Regulators spend countless hours interacting with all the components of the aviation ecosystem

- Once aircraft, facilities, or services operate under the State's oversight, the world can trust that assertion

Examples:

- Aerodromes
- Air Operators
- Aviation Maintenance Organizations
- Producers of aircraft, engines, propellers and parts
- Air Traffic Service Provision
- MET Service Provision
- AIS Service Provision
- Communication Facilities
- Design of aircraft, engines and propellers
- RVSM Monitoring Agencies
- Personnel
- **Remotely Piloted Aircraft Systems**
- **Unmanned Traffic Management (UTM)**
- **Upper class E Traffic Management (ETM)**
- **Future Autonomous Systems?**

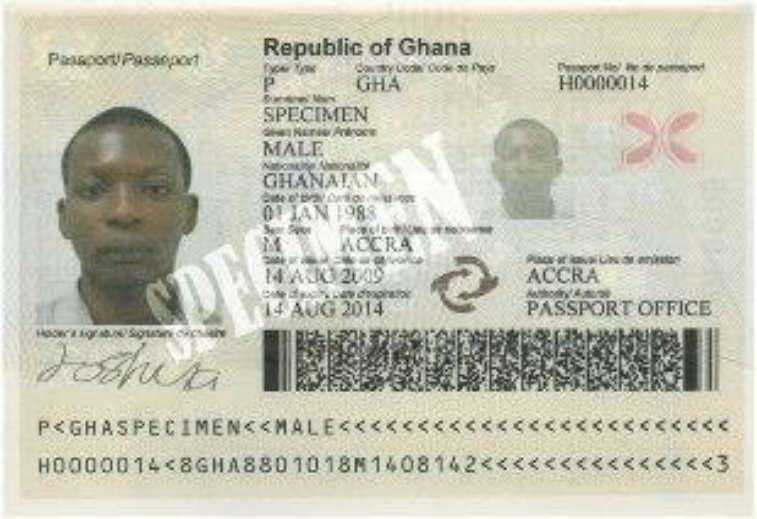
Which are its components?

- Digital Identity
- Network information security

Identity

- Provides information (**contents**) to answer the question “who/what are you?”
- Presents itself in a readable form (**credential**) that can be independently validated or proven, and carries a certain level of trust or recognition (**assurance**)

Example - Passport



- Is a **credential** that can be validated
- Has **contents** that describe the owner
- Provides a certain level of **assurance** the identity is valid

Digital Identity

- Digital identity is the digital equivalent of physical/personal identity
  - Says who or what you are
  - Provides a credential to validate
  - Asserts that credential to a given level of assurance

Digital Identity Usage

- Digital identity relies on easily usable, simple to validate and difficult to reproduce/forge **electronic credentials**

- Digital identity credentials have multiple uses:
  - Documents / Certificates for personnel and aircraft (ID badges, licenses, CoA, CoR, etc…)
  - Message validation (SWIM, ACARS Message Security, etc…)
  - Many, many more…

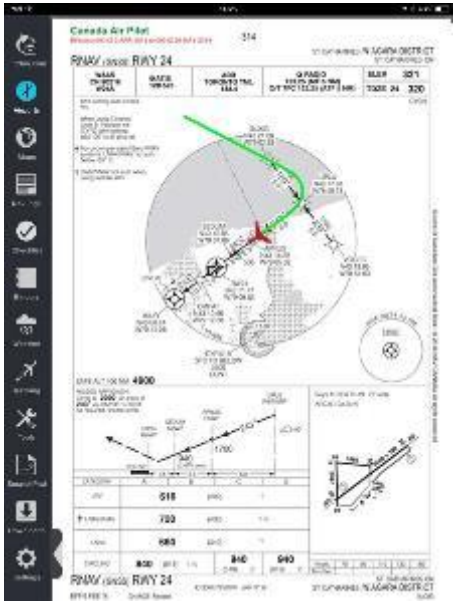
Digital Identity Usage

- Digital identity credentials must satisfy two basic requirements
  - The credential being presented can be validated as coming from its stated source
  - The information “digitally signed” using the credential has not been modified from its original form

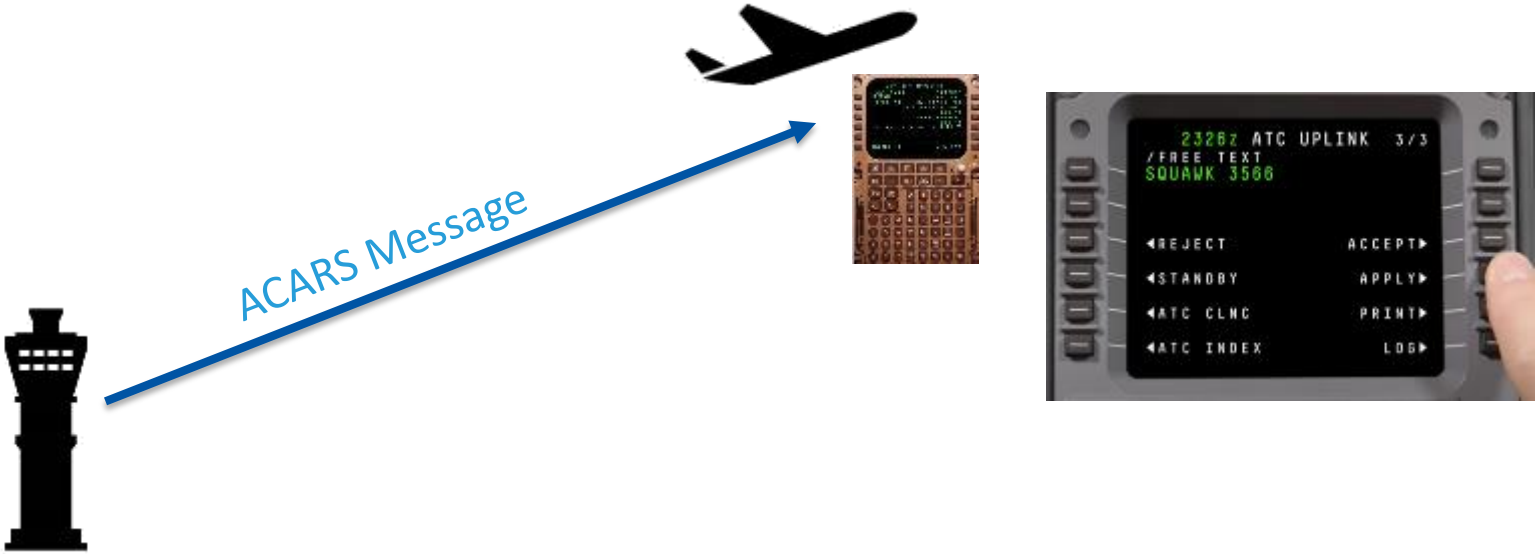
DI – Current Issues

- Absent a global mechanism, digital credentials from different entities are not interoperable with each other
- Each entity issuing digital identities can choose its own implementation path and what information to include in its credentials
  - Lack of universally harmonized digital identity credentials format/content for civil aviation
  - Each data field in the digital credential can vary between entities (Boeing-777 ≠ Boeing 777)
- Inconsistent implementation of existing technical requirements
  - Where standards exist, there is no global policy to enforce them uniformly and consistently
- Lack of harmonized identity/credential assurance criteria between entities
  - A “highly” trusted credential in one context may not be trusted in another

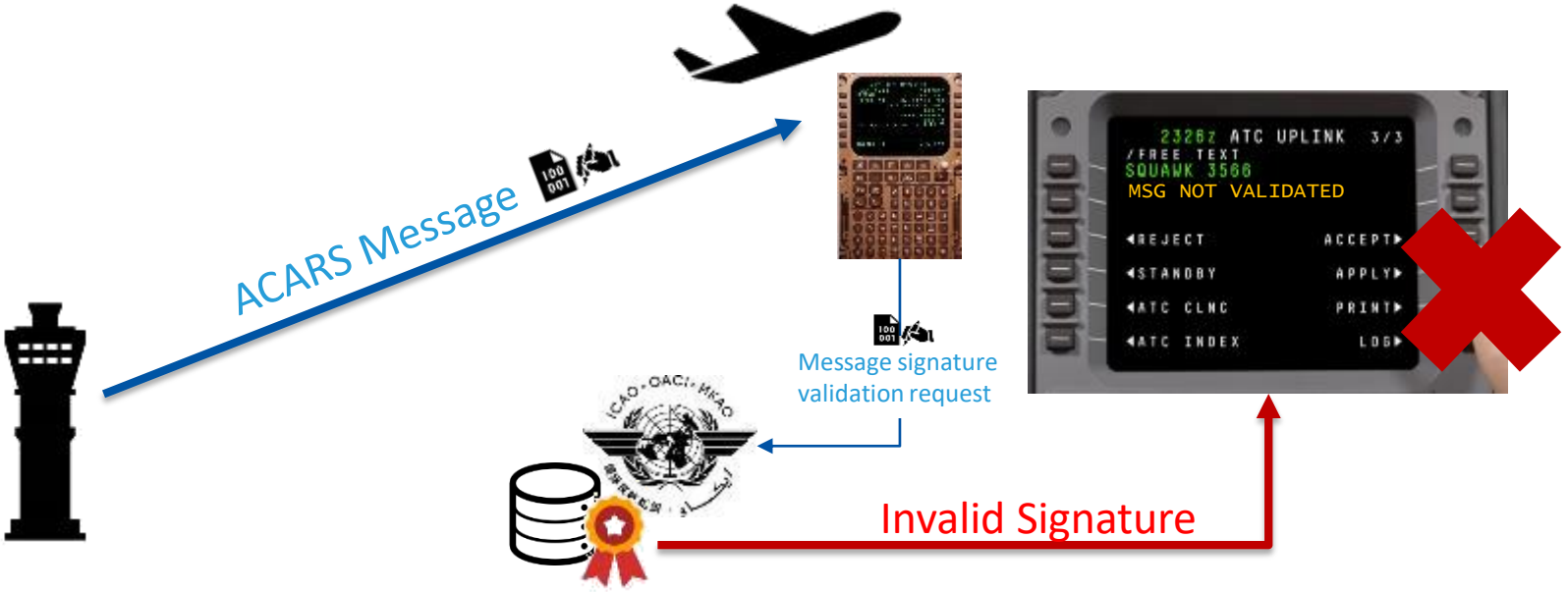
Are these valid?



Hypothetical Example



Hypothetical Example



Digital Identity Pillars

- Digital Identity enables interoperability & trust via four pillars:
  - Legal framework
    - Global basis for mutually recognizing credentials
  - Operations
    - Operational policies to enable mutual recognition of credentials
  - Technical requirements
    - Criteria that ensure interoperability of credentials
  - Oversight
    - Continuous monitoring and follow-up of credential issuers against legal and policy requirements

DI – Implementation Considerations

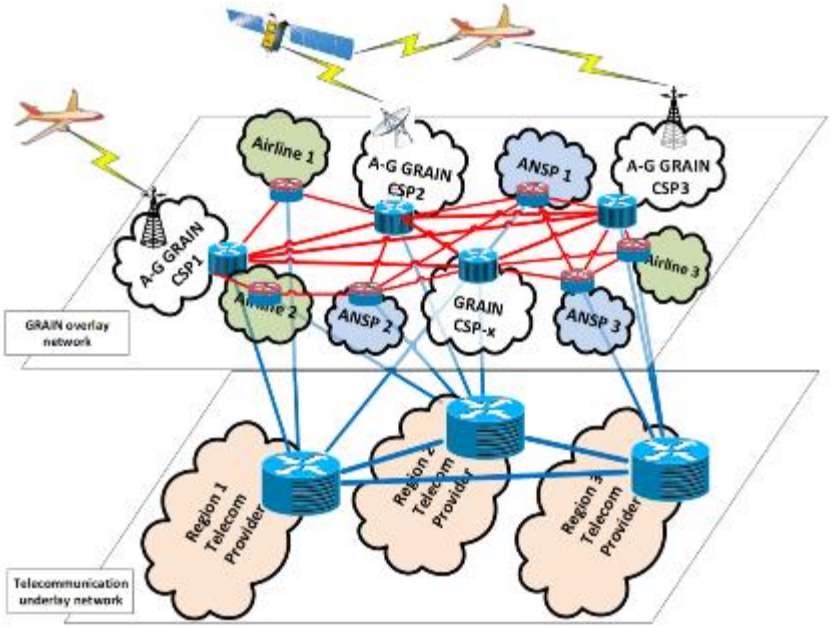
- Adoption of operational and technical policies and technical requirements
- Identity credential cross-recognition mechanism requirements
- Business process speed differences between aviation stakeholders (airframers vs drones)
- Consideration of legacy systems (forward-fit vs. retrofit)

DI – The Future

- Digital credentials from different entities are interoperable with each other through a global mechanism
- Standardized digital credential structures, formats and contents
  - Universally harmonized digital identity credentials format/content for civil aviation applications
  - Credential data fields based on ICAO-standard values (e.g. Doc 8643)
- DI technical standards applied consistently across aviation stakeholders
  - Even stakeholders not participating in the trust framework will base their digital credentials on ICAO requirements to ensure forward-fit compatibility
- Globally harmonized identity/credential assurance criteria between entities
  - Robust and proven assurance mappings widely available

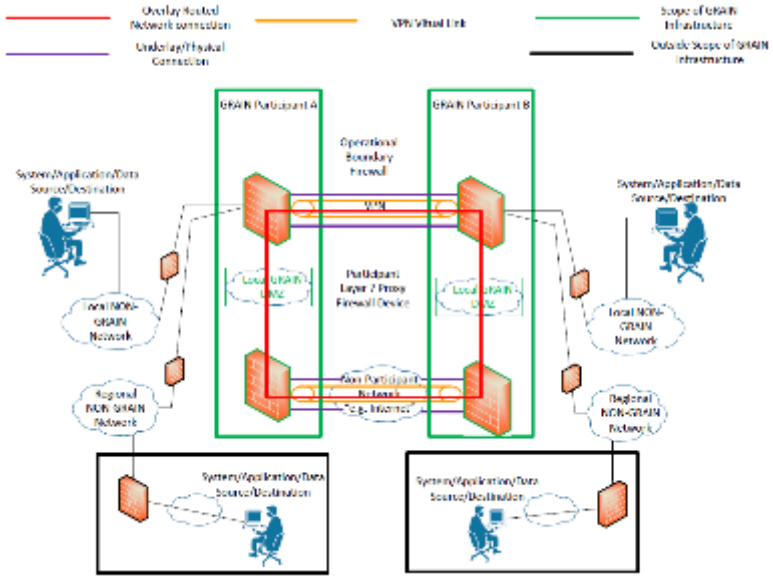
Network

- Virtual global network to connect regional and local aviation networks in a secure manner and provide for the necessary performance in the aviation system.



Network

- Technical requirements
  - IPv6 dedicated block
  - Domain Name System service requirements
  - Information security requirements
  - Network management requirements
  - Contingency plan requirements



Example IPv6 dedicated block

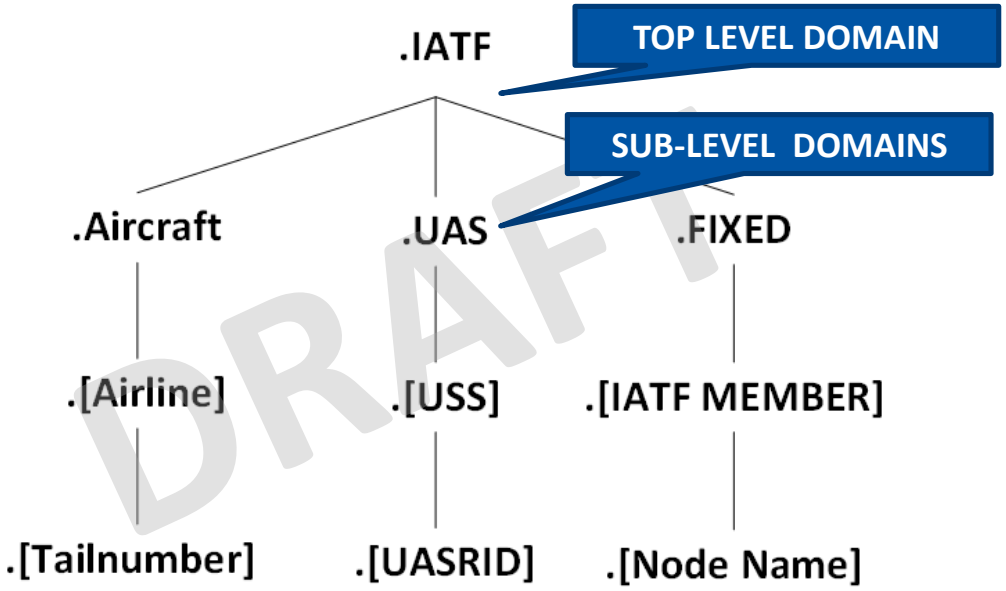
- Need for a dedicated IPv6 address block
  - Technical reasons (e.g. routing tables, SWIM)
  - Security layer (e.g. filtering)
  - Global recognition (e.g. allow aviation traffic)
- Develop a draft policy for the initial allocation and assignment of IPv6 addresses

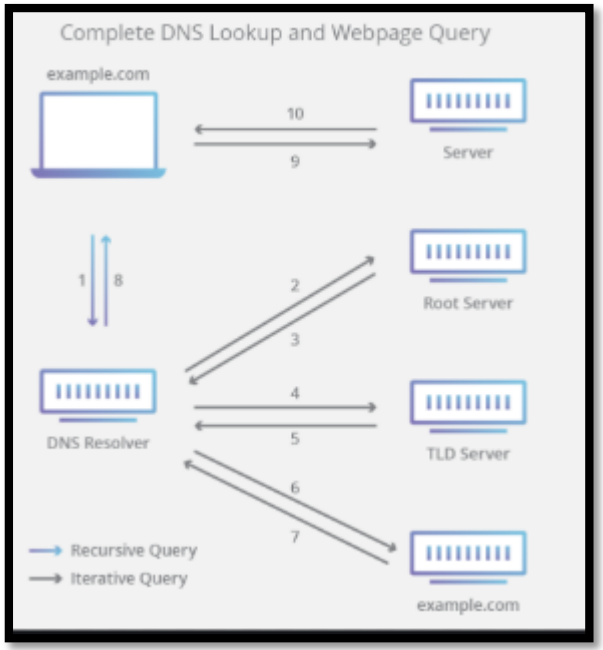
Example IPv6 dedicated block

/16 IANA Prefix Addressing Scheme of the largest estimated platform type

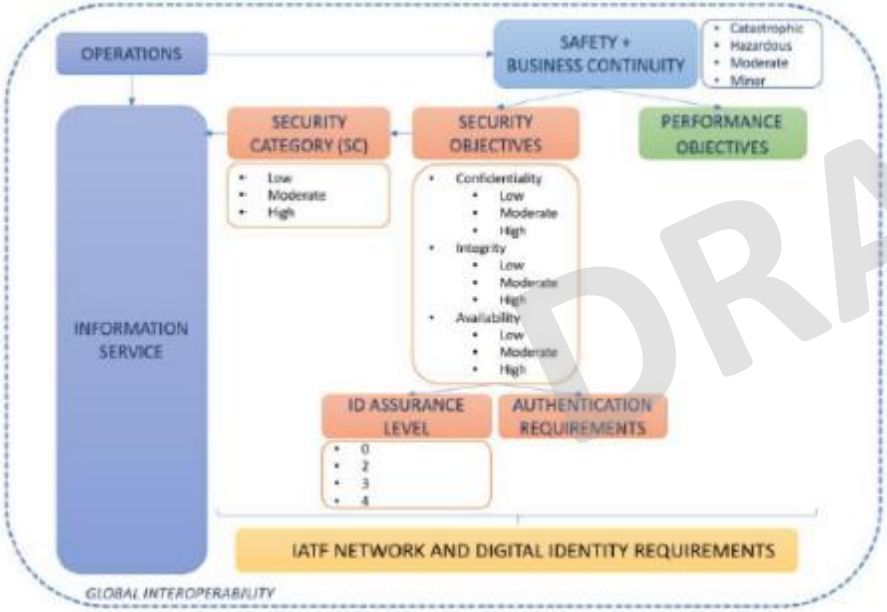
Bit #	Field Length	Purpose
1 – 16	16	ICAO IPv6 prefix
17 – 20	4	Platform type
21 – 28	8	States
29 – 38	10	USS per State (1024)
39 – 60	22	UAS per USS (4,000,000)
61 – 64	4	Subnets per UAS
65 – 128	64	Interface ID (per RFC 8064)

Example Domain Name System Service





Example Information Security requirement



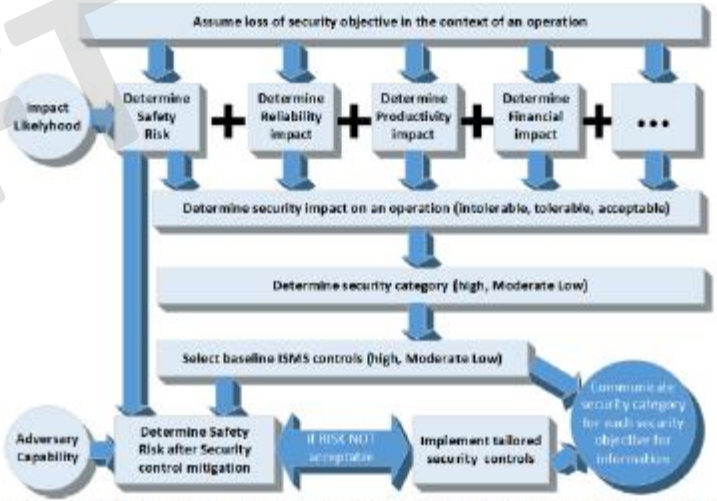


Figure 1 Process to determine the security category for information security objectives

Example Information Security requirement

Safety Risk Analysis (SRA) Risk Chart					
Minimum Capability Level	Novice/Intermediate				
	Proficient				
	Organized				
	Integrated				
	Institutionalized				
Total Risks:		Minor	Major	Hazardous	Catastrophic
		Safety Impact			

Safety Risk Level	Recommended action
INTOLERABLE	Take immediate action to mitigate the risk. Perform risk mitigation to ensure that additional or enhanced preventative controls are in place to bring down the safety risk level
TOLERABLE	Can be tolerated based on the security risk mitigation. It may rquire management decision to accept the risk
ACCEPTABLE	Acceptable as is. No further risk mitigation required

Figure 4 Information security safety risk analysis chart

SC information type = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}, where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

EXAMPLE 5: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. **SC** sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)}, and
SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

Example Information Security requirement

ID	Objective	Description	Type O= Organization T= Technical	Performance LOW	Performance MEDIUM	Performance HIGH	Security Triad C	Security Triad I	Security Triad A
3.0	**System Configuration and Management**								
3.10	Information Protection At-Rest	The entity shall implement cryptographic mechanisms to protect information at-rest		Systems shall protect information stored on hard disks with a minimum security strength of 128 bit. *Note: confidentiality protection means encryption*	Systems shall protect information stored on hard disks with a minimum security strength of 192 bit. *Not prot enc*	Systems shall protect information stored on hard disks with a minimum security strength of 256 bit.	X	X	

Control Mapping			
NIST 800-53	ISO 27001	ISO 27701	IATF CP
SC-28			

Example Network management requirements

- Monitoring of
  - Intrusion events
  - Security incident events
  - DDoS events
  - Anomalous traffic events
  - Outage events
  - Interface performance events
- Reporting of events

Figure 1 Shared Risk between Interconnected Aviation Stakeholders

Operations

- Management and allocation of IPv6 addresses
- Management of the domain name system service
- Run of the interoperability solutions lab
- Network monitoring
- Implementation of contingency plans

Oversight

- Auditors training and certification
- Auditing requirements
- Validation (independent validation? Self-validation?)
- Auditing escalation
- Audit report approval

CONCLUSION

- Trusted exchange of information is key to the future of the air navigation system
  - CNS/ATM systems and infrastructure must be ready to support trusted exchanges
- A global solution is necessary to enable universally accepted digital identities and end-to-end information security

ICAO

THANK YOU