CANSO

SHAPING OUR FUTURE SKIES

canso.org

CANSO activities on Cybersecurity

Eduardo García, CANSO Senior Manager Future Skiese

eduardo.garcia@canso.org

Who we are

Voice of Air Traffic Management

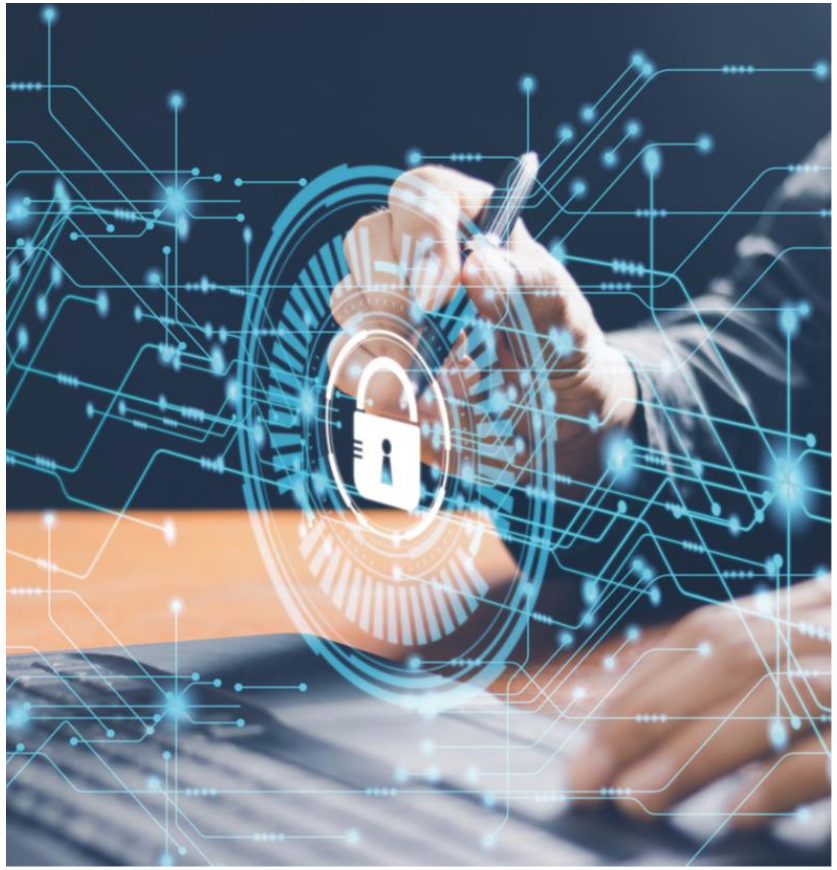
95 ANSPs

99 technology and other service providers

90% of world air traffic supported

Managing Safety-Critical Services in the Face of Agile Cyber Threat

Ensuring Resilience in an Era of Evolving Risks



Why It Matters

- Cyber threats now pose a greater and more frequent risk to critical services than technical failures.
- Modern protection strategies must go beyond prevention and include preparedness for rapid response.
- The continuity of safety-critical services requires proactive, layered defence and adaptive response.

Building a Robust Cyber Defence Strategy

Key Elements:

a. **Identify what is critical**: systems, resources, and processes essential for operations.
b. **Continuous monitoring**: real-time threat detection and adaptive protection.
c. **External cooperation**: with specialised cyber entities.
d. **Policy and audits**: regular updates, penetration testing, and policy reviews.
e. **Awareness & training**: foster a culture of cybersecurity through exercises and education.
f. **Risk management**: prepare business continuity (BCP) and disaster recovery (DRP) plans based on threat scenarios and asset vulnerability.

AI – A Double-Edged Sword in Cyber Defence

AI as a Support Tool

- Detects anomalies and predicts threats faster than traditional methods.
- Enables analysis of large data volumes in real-time.
- Enhances proactive responses to emerging cyber events.

Benefits:

- Early detection of irregular behaviours
- Faster incident response
- Enhanced predictive threat modelling

Threats:

- Adversarial AI used for advanced phishing or automated attacks
- AI systems exploited to find system vulnerabilities
- False sense of security from overreliance on automation

Cybersecurity in ATM: Regulatory and Contractual Challenges

- **Contractual Agreements**
  Challenges in incorporating cybersecurity requirements and associated costs into procurement and service contracts.

- **Legacy Systems**
  Feasibility of including contractual obligations for patching and mitigating vulnerabilities in ageing infrastructure.

- **Overregulation**
  Conflicting requirements from multiple supervisory authorities (often 3–4), creating complexity and inefficiencies.
  Does regulation truly bridge safety and security? Current implementation may fall short of this objective.

What we do

CANSO and its members seek to overcome challenges and harness opportunities in ATM by

Maintaining a network for global ATM experts

Leveraging global expertise to develop policies, positions and guidance to promote best practice in ATM.

Working with regulators, airlines, industry suppliers, airports and other aviation industry stakeholders.

Serving as the global voice of Airspace and represent the views of Members.

How we do it

Work programmes

- Operations
- Safety
- Strategy and Integration
- Future Skies

ICAO

Our Regions

Safety Programme

- **Safety Intelligence Workgroup (SIWG)** - identifies and measures global safety issues, hazards or risks. Seeks to advance data analysis and promotes the use of advanced analytical methodologies, tools and techniques. Collaborates with partners on global safety dashboard.
- **Human Performance Management Workgroup (HPMWG)** - helps ANSPs measure and improve human performance management (HPM) maturity and improve their effectiveness by supporting targeted assessments and workshops.
- **Cyber Safety Workgroup (CSWG)** - developing a cyber maturity model that focuses on how ATM prepares for, detects, responds and recovers from a cyber incident and provides guidance on cyber security risk assessment.
- **Next Generation SMS Workgroup (NexSMS)** - maintains the global Standard of Excellence in SMS for ATM and promotes new safety management concepts and methods.

Cyber Safety Work Group

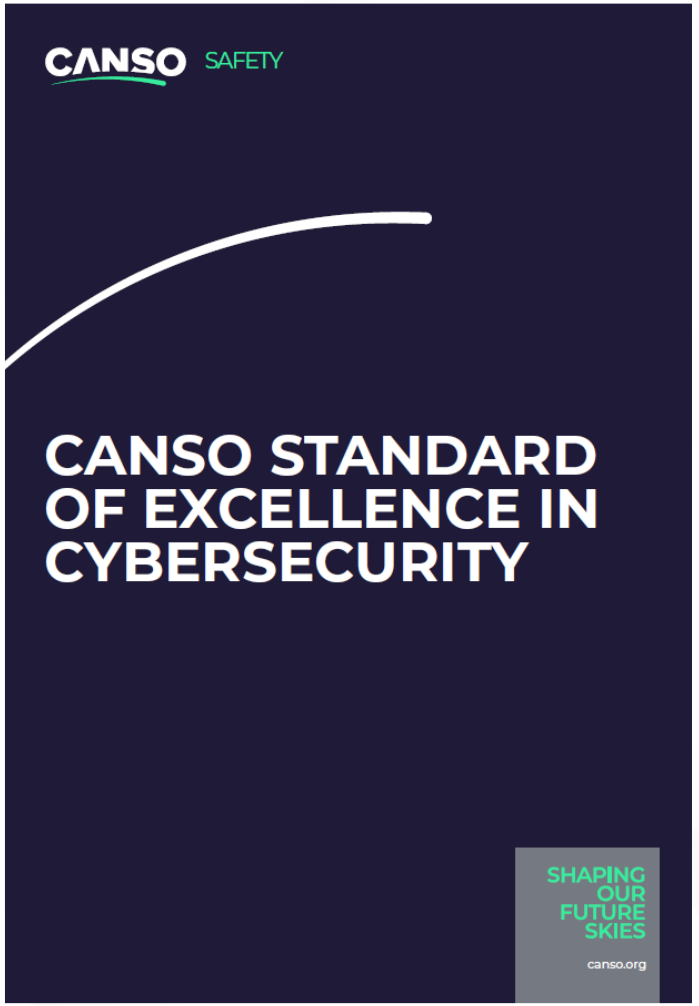
Primary mission is to develop a cyber maturity model that focusses on how the ATM service provider prepares for, detects, responds and recovers from a cyber incident, helping to ensure that ATM services remain safe during and following a cyber attack.

CANSO Standard of Excellence in Cybersecurity

The CANSO Standard of Excellence in Cybersecurity supports ANSPs by:

- Highlighting the critical elements of effective cybersecurity
- Allowing comparison of maturity levels either internally or externally, providing accessible, high-level summaries for management
- Facilitating a harmonised approach to cybersecurity across the ATM industry.

https://canso.fra1.digitaloceanspaces.com/uploads/2021/04/canso_standard_of_excellence_in_cybersecurity.pdf



CANSO

CYBERSECURITY EFFECTIVENESS

Level E – Optimised
Cybersecurity processes and/or requirements set international best practice, focusing on innovation and improvement. Feedback and improvement are embedded in the organisation. The effectiveness of the cybersecurity improvement actions is measured and evaluated against defined improvement criteria.

Level D – Assured
Evidence is available to provide confidence that cybersecurity processes and/or requirements are being applied appropriately and are delivering positive, measured results.

Level C – Managed
Cybersecurity processes and/or requirements are formally documented and consistently applied.

Level B – Defined
Cybersecurity processes and/or requirements are defined but not yet fully implemented, documented or consistently applied.

Level A – Informal Arrangements
Cybersecurity processes and / or requirements have not been agreed at the organisation level - they are either not routinely undertaken or depend on the individual assigned to the task.

CYBERSECURITY MATURITY

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Ident ity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B

Other CANSO Global Cybersecurity Activities

CANSO Emergency Response Guide

- The Guide helps ANSPs develop a formal emergency response plan that documents the orderly and efficient transition from normal to emergency operations and return to normal operations.

Contribution to ICAO activities

- Observer – Cybersecurity Panel (CYSECP)
- Member of the Trust Framework Study Group

Air Traffic Management Cybersecurity Policy Template

Purpose:

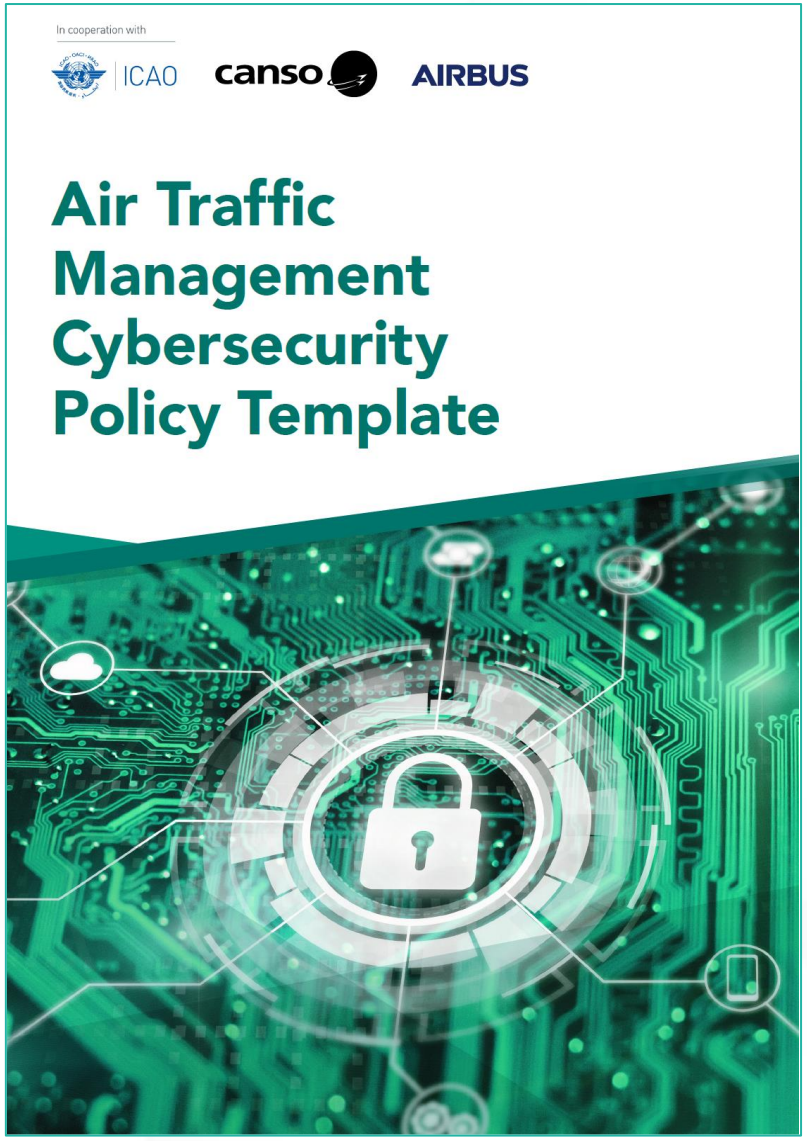
To help States implement robust cybersecurity mechanisms and foster a security culture across entire Air Traffic Management (ATM) systems and operations.

Key Objectives:

- Ensure aviation system resilience
- Safeguard information integrity, availability, and confidentiality
- Support civil aviation security, national defence, and law enforcement

A Living Document:The ATM Cybersecurity Policy Template evolves with emerging threats and technologies. Implementing it boosts organisational resilience and safety.

https://canso.org/publication/air-traffic-management-cybersecurity-policy-template/



TEMPLATE OF CYBER SECURITY REQUIREMENTS FOR USE IN THIRD PARTY CONTRACTS

This template document makes available a series of common security requirements which may be used by CANSO Europe and Borealis Alliance members when undertaking tendering processes in relation to operational products and services. The benefit of this document to the members is that, when presented to manufacturers and/or service providers at the earliest possible stage, these requirements may be considered and costed as initial requirements rather than as 'add-on features'as described by manufacturers/service providers which often result in an extra, increased cost.

The requirements have been set at a level that is not excessively technical but instead suitably high-level, thereby allowing the vendors to use their own skills and capabilities to establish the methods by which the requirements are met. Ultimately it will be for the customer to assess whether their requirements have indeed been met; this flexibility remains the right of the customer although this template will serve as the benchmark against which that assessment may be made.

The template document recognises that in some instances there will not be a clear basis upon which certification from an Internationally recognised Standardisation Body can be achieved. In order to support customers in this situation, a list of standards is included which may allow suppliers and/or service providers to demonstrate the existence of acceptable processes, practices, and procedures.

The template itself is considered to be a "living" document which will adapt and change through use in order to continually reflect best practice and experience.

January 2022

Cyber Safety Group – 2025 Workplan

Deliverables:

- How would ANSP return to service after a cyber attack
- Launch Slack Environment for internal communications.
- Create AI use guidance for ANSP's in cooperation with other WG's
- Host Ask Me Anything with Cyber leaders for all members
- Establish quarterly interviews w/Cyber luminaries and ANSP CISO's.

Complete Air
Traffic System
Global Council

CATS

CONOPS

For Future Skies

Why does ATM need to change?

Complete Air Traffic System Global Council

Capacity

What are the current limitations in ATM capacity, and how **soon** will we reach these limits?

Environment

How can improved ATM systems help reduce emissions and support sustainability targets?

Emerging airspace users

How might the integration of new airspace users push ATM systems beyond their current capabilities?

Safety/Security

Enhanced safety, security and resilience are non-negotiable as ATM becomes increasingly digital and data-driven.

OTHER ?

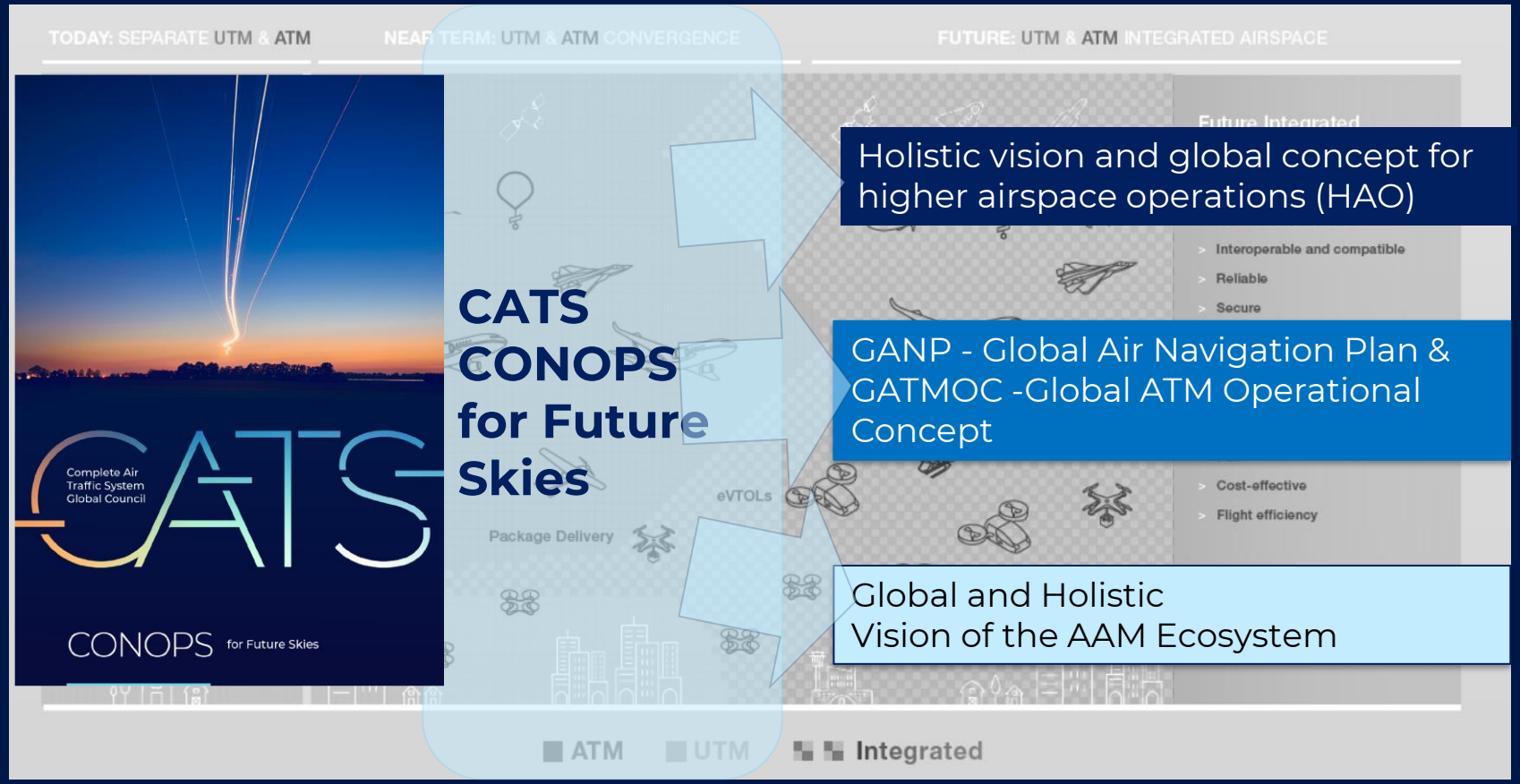
The CATS Global Council

Complete Air Traffic System Global Council

The CATS Global Council is an innovation forum of industry bodies, which believes that a shared blueprint and joint action are vital to make sure that future skies are efficient, clean and safe and can generate global economic prosperity and social

How is the CATS CONOPS going to be used?

Complete Air Traffic System Global Council



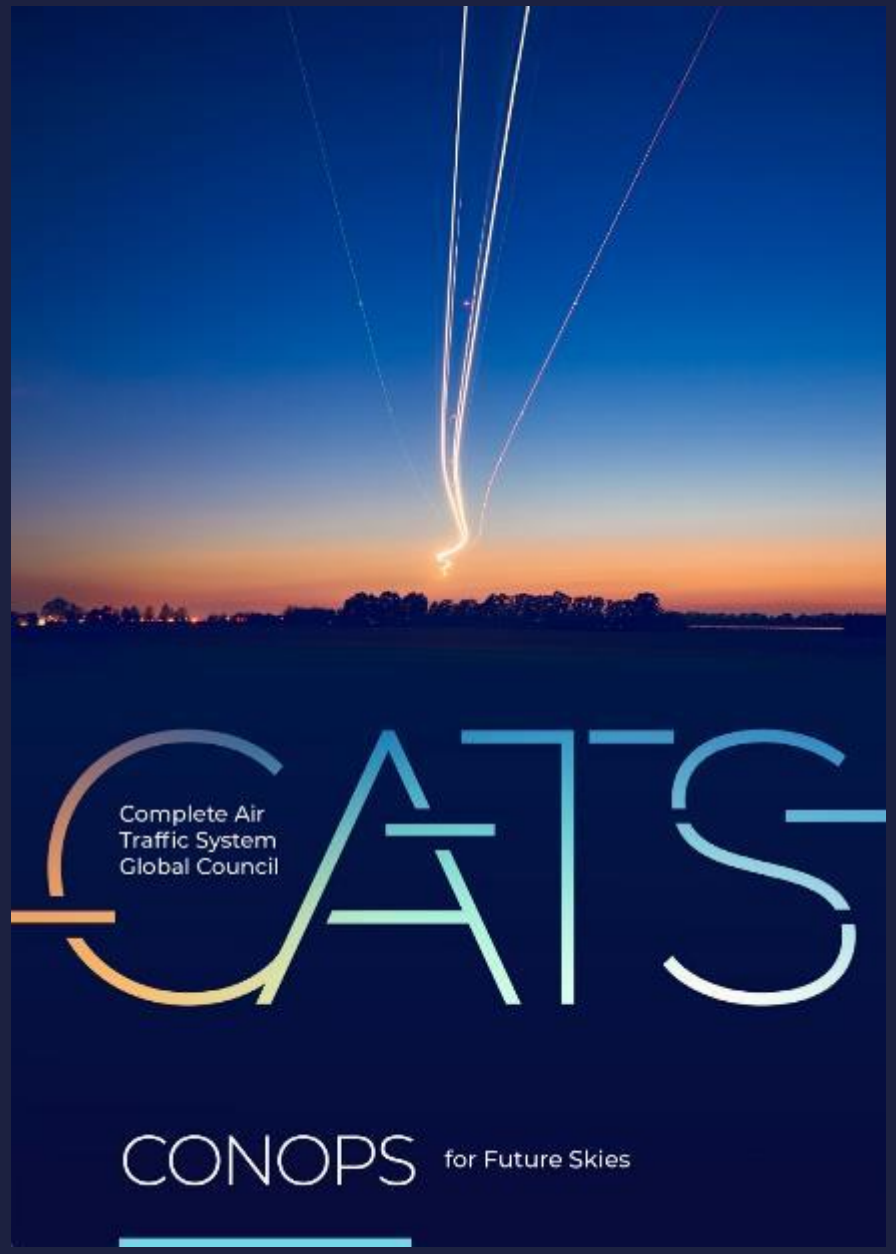
Holistic vision and global concept for higher airspace operations (HAO)

GANP - Global Air Navigation Plan & GATMOC -Global ATM Operational Concept

Global and Holistic
Vision of the AAM Ecosystem

Credit: Airbus & Boeing

ICAO • OACI • ИКАО
国际民航组织 • منظمة الطيران المدني الدولي



CONOPS

For Future Skies

CATS Complete Air Traffic System Global Council

A Key milestone!

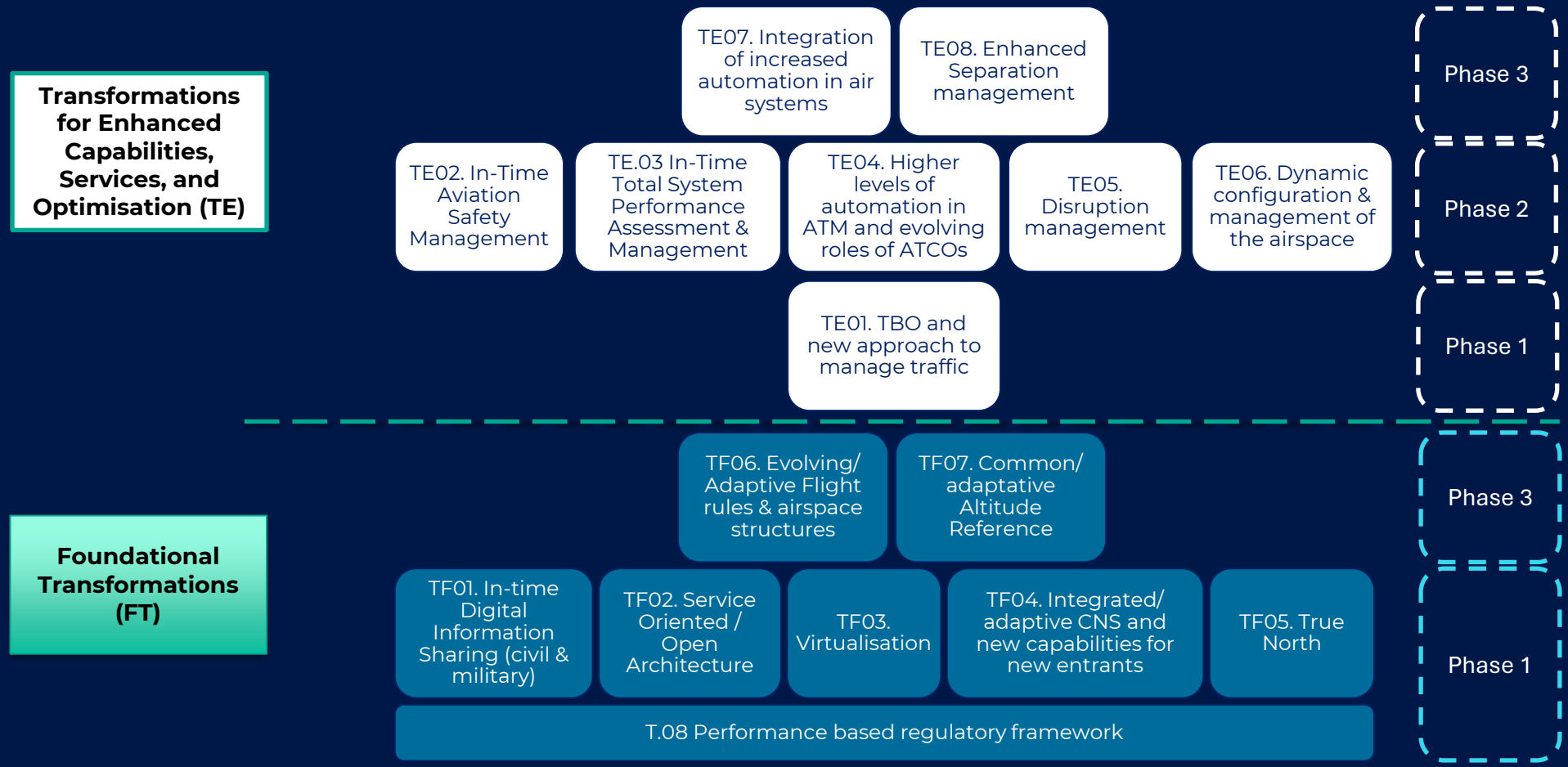
On 15 April 2025, CATS Global Council unveiled the CATS CONOPS for Future Skies, marking a significant step towards a seamless, sustainable, and scalable airspace by 2045.

https://www.futureskyvision.com/cats-conops

Key Transformations in ATM

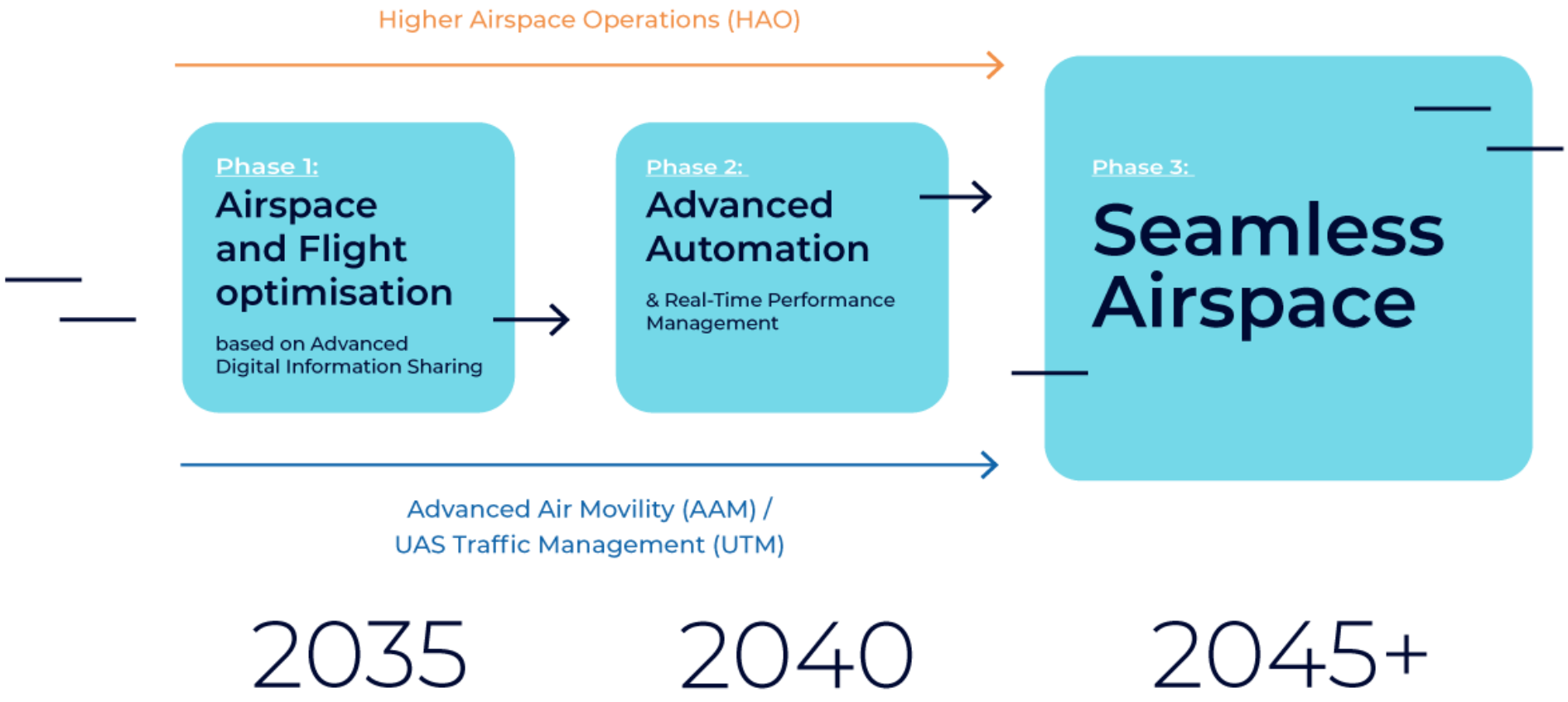
Complete Air Traffic System Global Council

"If we truly want to enable change, accelerate deployments and make a real difference, we need to focus and to set the right foundations now"



Pathway to Delivering the Future of Traffic Management

Complete Air Traffic System Global Council



Cybersecurity and Data Integrity

As digital information sharing expands, implementing robust cybersecurity measures becomes essential to safeguard aviation systems.

🛡️ Key Principles

- Zero-trust security: Assume no user or system is inherently trustworthy.
- Stringent data governance: Enforce strict rules on data access, handling, and integrity.
- Encrypted communications: Ensure secure transmission of sensitive data across all networks.

CANSO Key messages

- The current increase in geopolitical tensions has caused significant overhead and concerns amongst ANSP's because of our reliance on global digital interconnectivity. There is an urgent need to improve and support work under ICAO to improve our digital resilience.
- ANSP information sharing and cooperation should improve to deal with common threats and risks.
- We should consider common approaches towards security architecture and managing the supply chain, which would deliver efficiency and effectiveness benefits.

THANK YOU

eduardo.garcia@canso.org

CANSO

SHAPING OUR FUTURE SKIES