In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Introduction to cyber security policy for ATM

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Agenda

- **Introduction**
  - Security Benefits of Policy
  - Documentation
  - ***Developments in Cybersecurity in ICAO***
- **Introduction of Air Traffic Management Cybersecurity Policy Template**
  - Security policy template review
    - Goals
    - Content
- **Use case example**

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Introduction

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Security Benefits of Policy

How good security policy protects and defends

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Have we just been lucky so far…

- There have been security incidents that have affected aviation, but no truly disruptive cyber event.
- Is that because we're "good", or because we've been "lucky"

The "Good"

- We have a culture of care and attention to support safety
- Our systems generally operate in an isolated environment (but this is changing…)
- Our processes and procedures are naturally defensive & cautious
- We have checklists of checklists

What if…

- … our safety focus can be used to distract from other threats
- … the systems we trust implicitly have been altered
- … our caution stops us acting quickly when we need to
- … our checklists & procedures make us predictable to an attacker
- … a supplier we trust gets compromised

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

CASE STUDY: SOLARWINDS "SUNBURST" ATTACK

Probably the most publicised attack so far in 2021

In late 2020, SolarWinds discovered malicious code had been inserted into its Orion monitoring product.

The malicious code was distributed to customers around March 2020.

The attackers first accessed internal SolarWinds systems in Sept 2019.

Information taken from Microsoft Security's Deep Dive into Solorigate/SUNBURST[1]

Step 4 - Compromise

The code was designed to provide an entry point into end user organizations. **Even in isolated environments.**

Step 3 - Deployment

The attackers deployed 4,000 lines of malicious code, packaged as a genuine part of Orion

Step 2 - Research

The attackers spent time researching the protections SolarWinds had in place and finding a way to use them maliciously.

Step 1 – Unauthorized Access

The attackers covertly found a way into SolarWinds' systems and established a persistent capability.

Source:
1] https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop

WHY USE "POLICY" AS A SECURITY CONTROL?

But isn't security about technical protections, firewalls and keeping 10,000 unique passwords?

These technical protections need to build on a solid foundation:

Risk Management

Business is about **managing risk**, so this is about managing security in a way that is familiar and well understood.

Regulation

Aka **Governance** – independent oversight to help keep the right behaviours happening.

Maintenance

Protecting against **supply chain** attacks via maintenance partners

Comms Security

Protecting against **impersonation** and **being influenced** by anonymous attackers

Handling Incidents

Consider an incident might be an **intelligent attacker** rather than a statistical event.

Think about **Business Continuity**, maybe graceful degradation of service.

Also consider **Disaster Recovery** – how to rebuild from nothing.

Share knowledge and **work together** - even commercial competitors are on the same side against attackers.

New Systems

Design in **foundational security**, and make sure **procurement chains** are trustworthy and not compromised

Access Control

Both **physical** and **logical**, use of least privilege, etc.

Ops Security

Building good cyber into operational processes

Compliance

Maintaining **evidence packs** – a key part of Audit

Asset Management

Knowing what you have, and what vulnerabilities you might be exposed to

Policy stands as the foundation of good technical protections

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Is There any Example For "Good" Policy

Of course! The "Air Traffic Management Cybersecurity Policy Template"

Developed in partnership by ICAO, CANSO and Airbus:

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

CONTEXT

Risk Management:

- Consider security throughout all risk management
- Have a methodical process to give justifiable decisions
- Integrate security across the entire lifecycle

Asset Management:

- Know what you have
- Control access and be proportionate to IT/OT/IACS/Comms
- Recognise the value of data as well as physical assets

Supply Chain:

- Map the entire end-to-end chain
- Start at adjacent links and work out
- Mitigate using Risk Management

Incident Response:

- Prepare and consider Informed Attackers
- Define priorities based on scenarios
- Share information with partners

OBJECTIVES

Risk Management & Governance

- Management SECTION 7
- Regulation SECTION 8
- Compliance SECTION 20

Protecting Assets

- Asset Management SECTION 10
- Operational Security SECTION 13
- Access Control SECTION 11
- Communication Security SECTION 14

Supply Chain

- Maintenance SECTION 15
- Acquisition SECTION 15
- Relationships SECTION 16

When things go wrong...

- Incident Management SECTION 17
- BC / DR SECTION 18
- Speaking out SECTION 18

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

So What are the benefits

- Looking back over the how the ATM Cyber Policy Template requirements protect against an attack like the SolarWinds Orion attack…

Access Control

Comms Security

New Systems

Ops Security

Maintenance

Handling Incidents

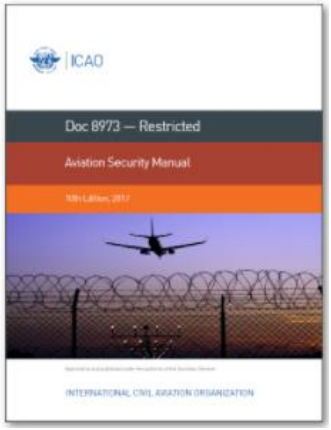
In cooperation with

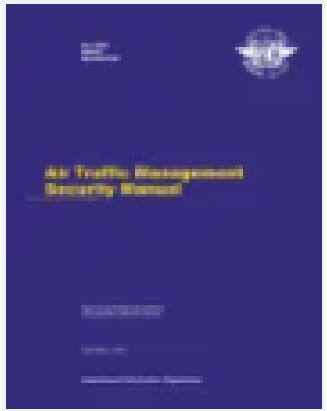
ICAO

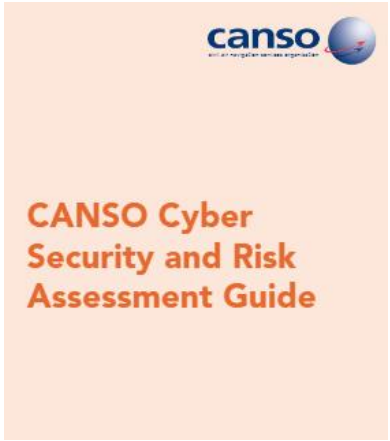
canso
civil air navigation services organisation

AIRBUS

Documents







In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Documentation

- *Resolution A40-10: Addressing Cybersecurity in Civil Aviation*
- *Air Traffic Management Cybersecurity Policy Template.*
- *Safety Management Manual (SMM) (Doc 9859).*
- *ICAO Aviation Security Global Risk Context Statement (Doc 10108)*
- *Aviation Security Manual (Doc 8973)*
- *Annex 17: Security Provisions*

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Documentation

- *Air Traffic Management Security Manual (Doc 9985)*
- *Annex 19; Safety Management.*
- *ICAO Aviation Cybersecurity Strategy*
- *CANSO Standard of Excellence in Cybersecurity*
- *ISO/IEC 27000-series comprises information security standards*
- *ICAO Cybersecurity Action Plan*

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

ISO/IEC 27000-series comprises information security standards

- Information about best practices to improve information security
- ISO/IEC 27000 Information security management systems Overview and vocabulary
- ISO/IEC 27001 Information security management systems Requirements
- ISO/IEC 27002 Code of practice for information security management
- ISO/IEC 27003 Information security management system implementation guidance
- ISO/IEC 27004 Information security management Measurement
- ISO/IEC 27005 Information security risk management
- ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27010 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

ISO/IEC 27000-series comprises information security standards

Information about best practices to improve information security

- ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031 Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27033-1 Network security overview and concepts
- ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
- ISO/IEC 27035 Security incident management
- ISO 27799 Information security management in health using ISO/IEC 27002

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cybersecurity must interface with other disciplines (safety, efficiency) similarly to what currently happens with “traditional” aviation security to ensure the accurate assessment of exposure to cybersecurity threats and ensure the development of effective and efficient risk-based cyber-protection strategies. Cybersecurity needs to build bridges between aviation security and safety as the multi-disciplinary nature of cybersecurity needs to benefit from security and Safety.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Developments in Cybersecurity in ICAO

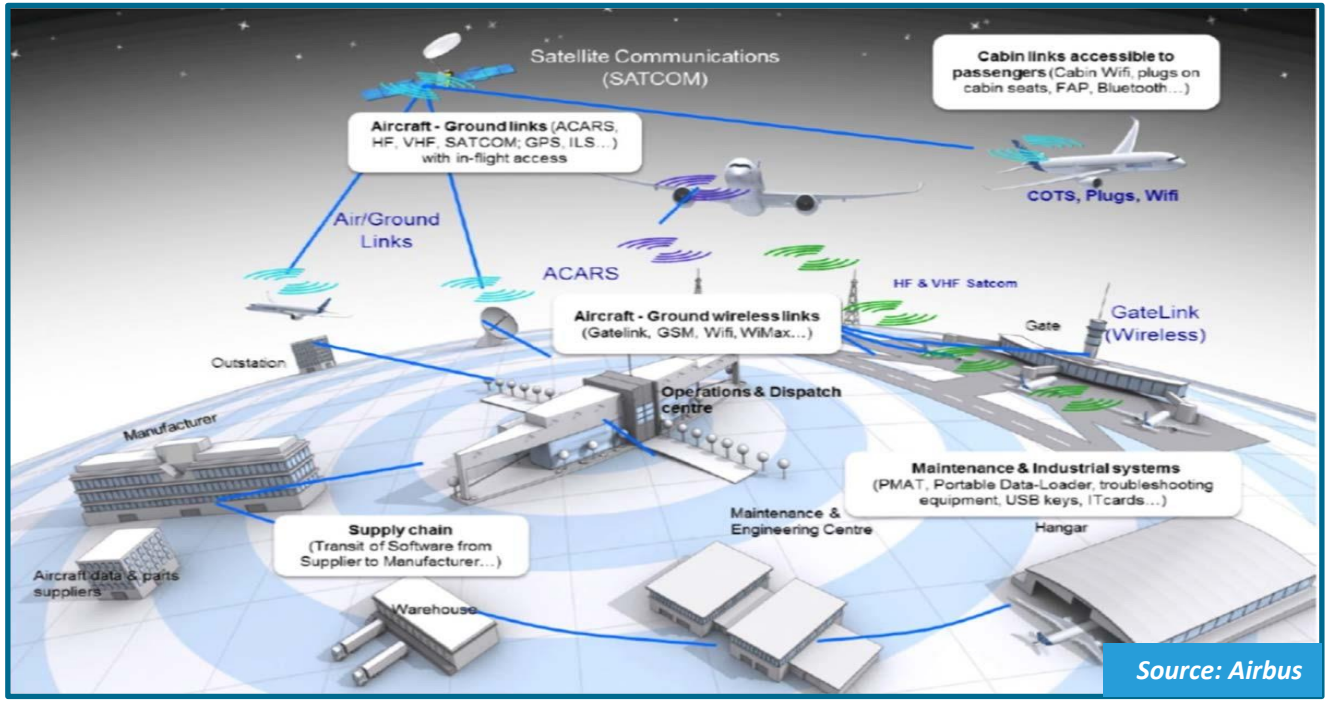
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Why Cybersecurity in Civil Aviation?



Source: Airbus

Inter-connection & Inter-operability of Digital Systems between Aviation Stakeholders Expands the Cyber Threat Landscape

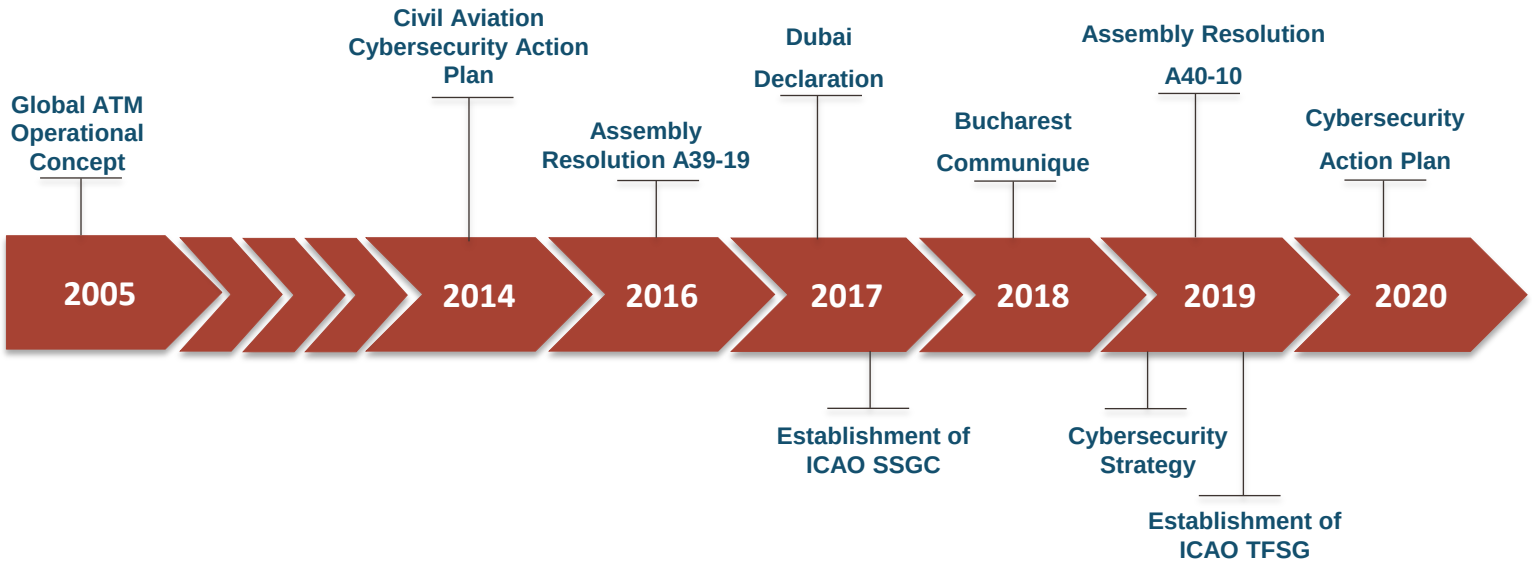
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

ICAO Cybersecurity Timeline



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

ICAO's Work on Cybersecurity

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity
- **Standards and Recommended Practices:**
  - Annex 17 – *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Guidance Material:**
  - Procedures for Air Navigation Services – PANS
  - Doc 8973 – *Aviation Security Manual*
  - Doc 9985 – *ATM Security Manual*
  - Aviation Cybersecurity Strategy
  - Cybersecurity Action Plan
- **Training**
  - Cybersecurity Training Roadmap
  - Training Courses

In cooperation with

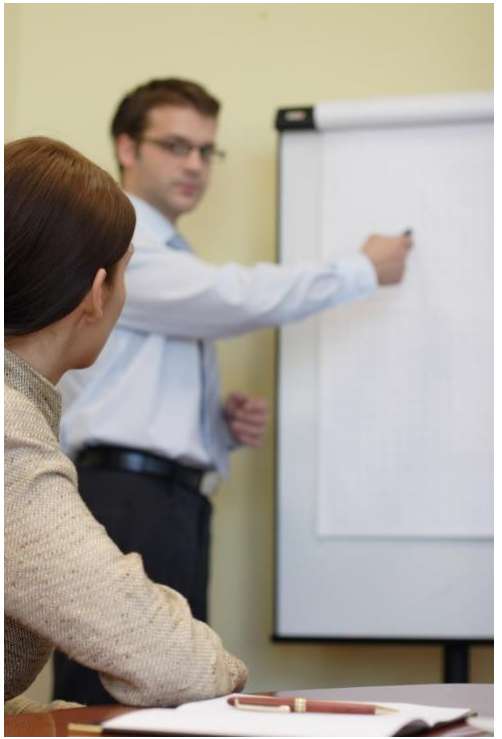
ICAO

canso
civil air navigation services organisation

AIRBUS

Training

- **Training Courses in the Pipeline:**
  - ✓ Foundations of Aviation cybersecurity Leadership and Technical Management
    - ✓ Developed in Partnership between ICAO and Embry-Riddle Aeronautical University
    - ✓ Two Tracks: Leadership & Technical Management
  - ✓ Managing Security in ATM
    - ✓ Developed in Partnership between ICAO and EuroControl
    - ✓ Covers Traditional ATM Security as well as Cyber.



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Expert Groups within ICAO Addressing Cybersecurity in their Work

- **Secretariat Study Group on Cybersecurity – SSGC**
  - ✓ Research Sub-Group on Legal Aspects
  - ✓ Working Group on Airline and Aerodromes
  - ✓ Working Group on Air Navigation Systems
  - ✓ Working Group on Cybersecurity for Flight Safety
- **Trust Framework Study Group – TFSG**
  - ✓ Trust Reciprocity Operational Needs Working Group
  - ✓ Digital Identity Working Group
  - ✓ Global Resilient Aviation Interoperable Network Working Group

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Feasibility Study on the Mechanism to Address Cybersecurity in ICAO

- Work began in 2018.
- First Draft Presented to Council in 2020.
- Small Working Group (SWG)
  - Established on 30 October 2020
  - Met 15 times between in less than two months
  - Developed 3 Options, Evaluated them, and Recommended a preferred option for Council's Consideration

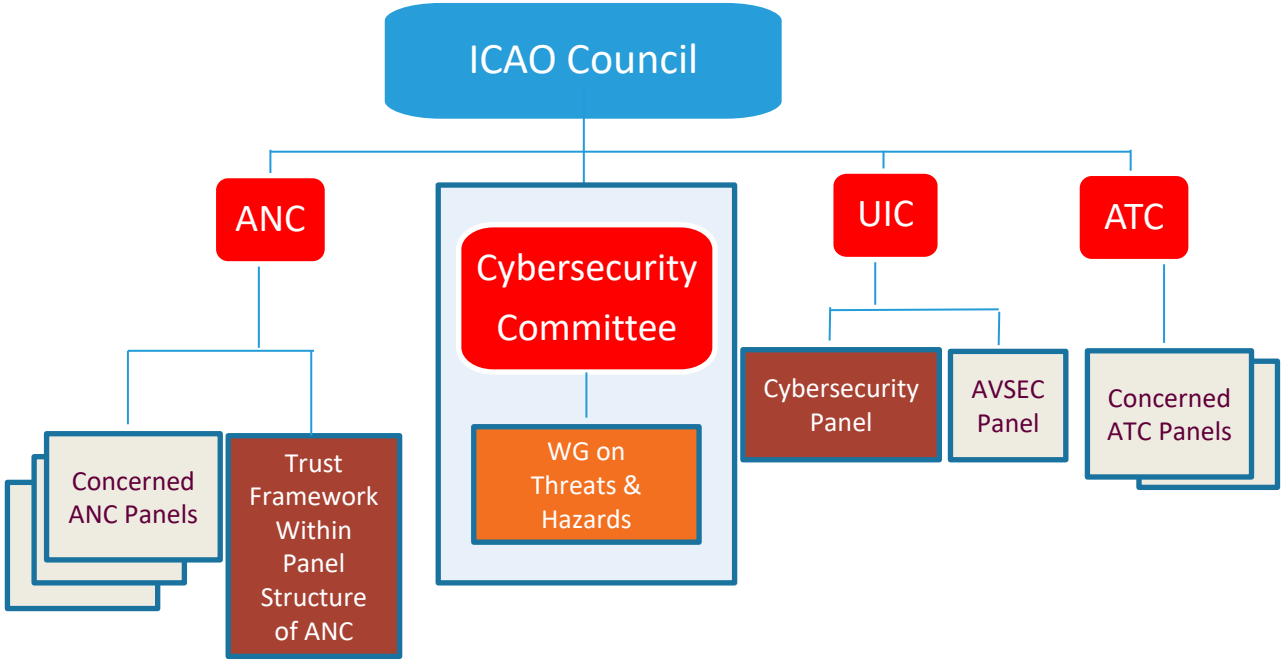
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Council's Decision on the Mechanism to Address Cybersecurity in ICAO



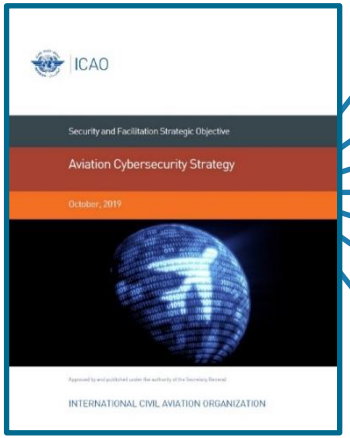
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Aviation Cybersecurity Strategy



- International Cooperation
- Governance
- Effective Legislation & Regulations
- Cybersecurity Policy
- Information Sharing
- Incident Management & Emergency Planning
- Capacity Building, Training, & Cybersecurity Culture

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Cybersecurity Action Plan

- Published in November 2020.
- **TLP Green**.
- **Provides the Foundation** for ICAO, States and stakeholders to work together, and proposes a **Series of Principles, Measures, and Actions** to achieve the objectives of the Cybersecurity Strategy's seven pillars.
- **Develops the Seven Pillars** of the Aviation Cybersecurity Strategy into **29 Priority Actions**, which are further broken down into **54 Tasks** to be Implemented by ICAO, States, and Stakeholders.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Cybersecurity Action Plan (Example)

Priority Outcome	Pillar 3: DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS
Priority Actions	• Ensure that appropriate regulation and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and Industry in implementing cybersecurity related provisions; • Ensure that international legal instruments provide appropriate measure for the prevention, timely reaction to, and prosecution of cyber-incidents.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability in Action Plan	Specific Measures/Tasks	Indicators	Maturity	Target
CyAP 3.1	Member States	3.3	8.4	Member States to ratify Beijing instruments.	Number of States having ratified Beijing instruments	Low	ongoing
CyAP 3.2	ICAO	3.3	8.3	Analysis of international air law instruments	Report and update plan	N/A	2020
CyAP 3.3	ICAO and Member States	3.3	8.2	Analysis of existing international and national legislation in the cybersecurity field and identify gaps, including criminal law.	Promote ratification of instruments to incriminate unlawful cyber acts.	Medium	2022 - 2023
CyAP 3.4	ICAO, Member States and Industry	3.3	8.1	Review existing ICAO security standards to identify need for potential cybersecurity updates	Regulatory gap analysis	High	2021
CyAP 3.5	ICAO	3.2	5.4	Create, review and amend guidance material related to implementing cybersecurity requirements	Accepted and agreed cybersecurity guidance material	High	2021-2022

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Introduction of Air Traffic Management Cybersecurity Policy Template

In cooperation with

ICAO

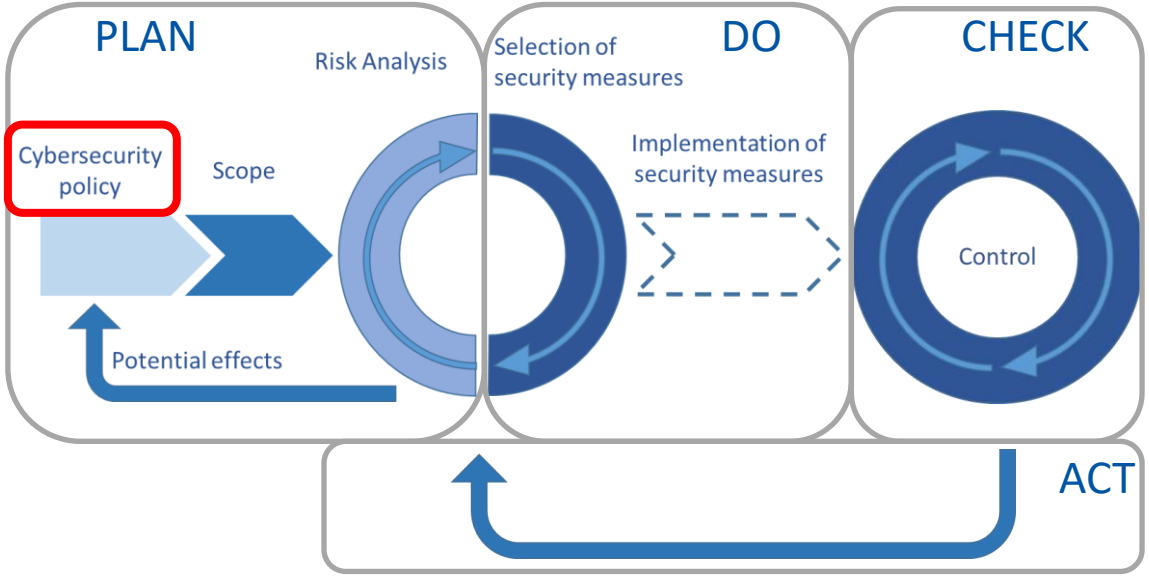
canso
civil air navigation services organisation

AIRBUS

Information Security Management system (ISMS) approach

ISMS provides a systematic approach for managing an organization's information security.

- With the objectives to:
  - Comply with safety constraints
  - Provide resilience
  - Ensure reliability
  - Support ATM business model



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cybersecurity policy for setting up ISMS

Requirement ATMSP-001-01

Based on this security policy, an information security management system shall be defined, implemented and maintained based on a risk management approach.

NB: ISO27001 and ISO27002 Standards provide approved process and best practices for ISMS Benefits from Airbus Aircraft Security Management System principles

➔in addition: achieving maturity enables reducing too many changes to System and Information Systems under safety regulation constraints (Cost driven)

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cybersecurity policy objectives

- Focused on 2 key objectives
  - Safety
  - Business continuity
- Based on ISO27001 and IEC62443 (industrial systems) key principles
- Benefits from Airbus Aircraft Security Management System principles

➔ To provide consistent end-to-end security: “security by design from ground to air”

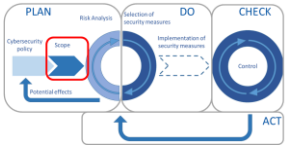
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Scope & Objectives



- Address the whole ATM:
  - Actors, employees, partners and suppliers
  - Services and related information systems
  - Infrastructures (IT, OT, IACS)
- With the objective to provide resilience
  - Based on criticality regarding safety and operability

Infrastructures (IT, OT, IACS)

IT Infrastructure	OT & IACS Infrastructure
IT infrastructure are the components required to operate and manage enterprise IT environments. hardware, software, networking components, an operating system (OS), and data storage.	Operational Technology (OT) and Components Cybersecurity Certification Scheme; Industrial Automation & Control Systems (IACS). Critical element for cybersecurity

Cyber security Risk Management

Requirement ATMSP-002-01:

ATM security shall be intelligence led, threat based and risk managed.

Requirement ATMSP-003-01:

Information security risk management shall be considered as an integral part of the overall system life cycle process.

Cyber security Risk Management

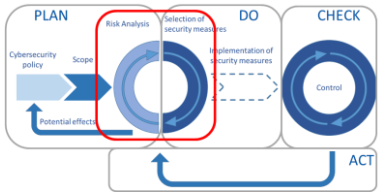
Requirement ATMSP-004-01:

All ATM assets (data, systems, personnel…) shall have defined ownership.

Requirement ATMSP-005-01:

Defense in depth principles as defined in 5 – Security architecture objective, shall be part of the information security management.

Cyber security Risk Management



Requirement ATMSP-006-01:

ATM Security Risk based approach shall implement technical security measures and operational security measures (policies and processes) to reduce risk to an acceptable level regarding:

- (Intentional) Successful cyber-attack,
- Human error,
- Accident or incident,
- Impact from natural disaster.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cyber security Risk Management

Requirement ATMSP-007-01:

The organization in charge of physical or information ATM security shall ensure efficient and coordinated treatment of security risk.

Requirement ATMSP-008-01:

ATM information security risks shall be reviewed and monitored on a regular basis.

Cyber security Risk Management

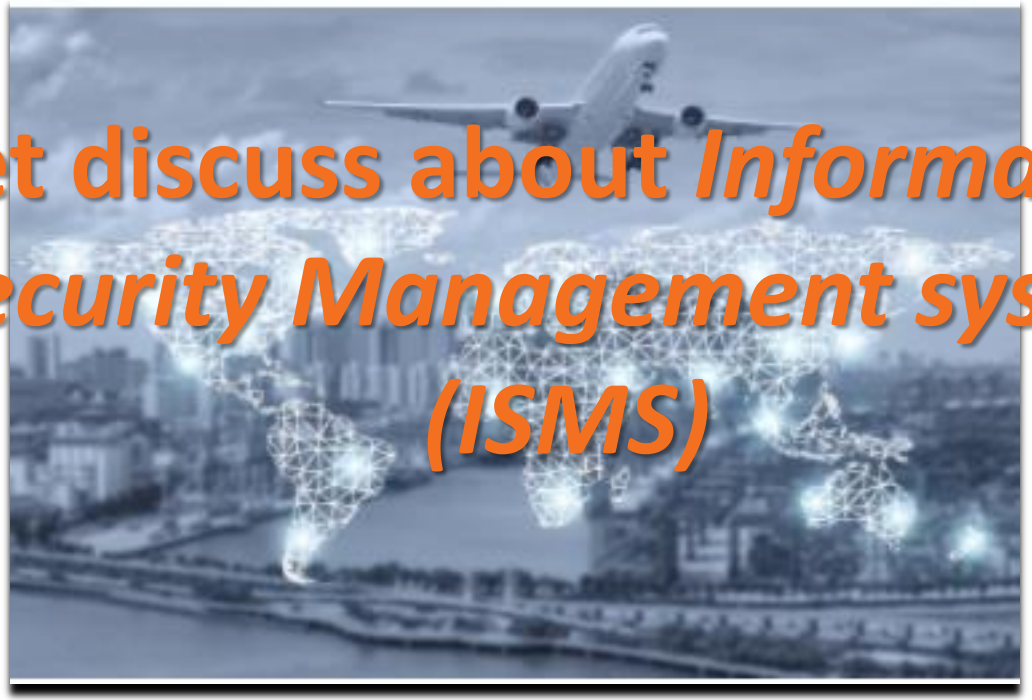
- Reduce risk to acceptable level
  - Based on criticality regarding safety and operability
- Likelihood based on systems' resilience to the Attack
  - Architecture principles
  - No single nor common point of vulnerabilities

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS



Let discuss about *Information Security Management system (ISMS)*

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Security Governance and Organisation

Requirement ATMSP-009-01:

CAA shall designate the Appropriate Authority (AA) responsible for the overall ATM security.

Requirement ATMSP-010-01:

CAA designated ATM security responsible shall define at a minimum:

- Roles and responsibilities for ATM security risk management;
- Process for risk management;
- Processes for incident, crisis and business continuity management.

Requirement ATMSP-011-01:

Skills and competencies of personnel appointed to ATM security roles and responsibilities shall be kept up to date.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Security Governance and organization

- Think cybersecurity on long term perspective
  - Cybersecurity policy in place and applicable
  - Cybersecurity identified as core stake of the organization (as for safety)
- Define Roles and Responsibilities
  - Formal nomination
  - Detailed description of responsibilities


Security risk

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Policy in details

- Human resources
- Asset management
- Access control
- Physical and environment security
- Operation security
- Communication security
- System Acquisition, Development and Maintenance
- Suppliers and partners
- Security Incident Management
- Business continuity
- Personal data
- Compliance

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Human resources

- Background check before employment
- Security culture and training during employment
- De-provisioning and commitments reminders after employment

Human resources

Requirement ATMSP-012-01:

Personnel shall be part of ATM security during all employment phases:

- Before employment: through measures such as background checks in accordance with local regulations;
- During employment: by developing a security culture through regular training and raising awareness; and
- After employment: by ensuring the respect of the de-provisioning process and reminding staff of non-disclosure commitments.

Human resources

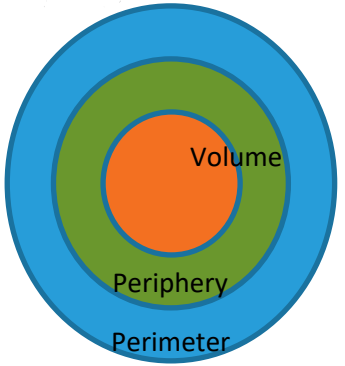
Requirement ATMSP-013-01:

Security personnel shall ensure that individuals with access to ATM facilities, controlled areas and ATM sensitive data do not constitute an unacceptable risk (as per Chapter 7 Risk Management).

security background checks

Asset management

- Set up and maintain asset inventory
- Include criticality (regarding safety and operability) in assets' categorization
- Ensure consistency between
  - Logical and physical access
  - Access and zoning



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Asset management

Requirement ATMSP-014-01:

An inventory of ATM assets shall be developed and kept up to date.

Requirement ATMSP-015-01:

ATM shall classify (categorize) its assets according to their criticality in order to implement appropriate means of protection.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Asset management

Requirement ATMSP-016-01:

ATM data shall be by default classified with adequate level of classification.

Additional information: please refer to applicable national regulation

Requirement ATMSP-017-01:

ATM data shall be protected during storage, processing and exchange, in line with its sensitivity profile.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Let talk about cybersecurity asset

Logical zoning

- Zoning is a logical design approach used to control and restrict access and data communication flows only to those components and users as per security policy.

In cooperation with

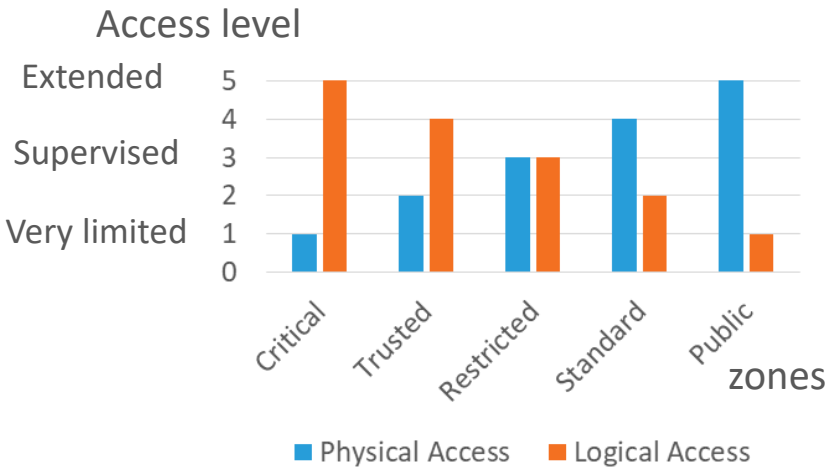
ICAO

canso
civil air navigation services organisation

AIRBUS

Access control & Physical and Environmental Security

- Pay attention to the balance between physical and logical access control
- Ensure consistency of logical and physical zones
- Monitor and adapt to changes
  - Regular checks and revisions
  - Disposal & decommissioning



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Access control & Physical and Environmental Security

Requirement ATMSP-018-01:

Access to any ATM assets shall be granted on:

The verification of absence of unacceptable risk (as per Chapter 7 Risk Management);

need-to-know basis).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Access control & Physical and Environmental Security

Requirement ATMSP-019-01:

ATM physical security shall safeguard IT, OT, IACS and CNS/ATM infrastructure, against unlawful interference and unauthorized access.

Requirement ATMSP-020-01:

ATM physical security shall identify zones hosting CNS/ATM assets according to their criticality regarding safety and operability.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Access control & Physical and Environmental Security

Requirement ATMSP-021-01:

ATM physical security measures shall protect the CNS/ATM from unlawful or intentional interruption of services and operations.

Requirement ATMSP-022-01:

ATM physical security shall protect incoming and outgoing flows from storage zones and data centers.

Cybersecurity zones

Operation Security

- Operate security from trusted zone
- Efficiency of security measures based on robustness of security processes
- Apply vulnerability management process (including monitoring, qualification and mitigation)

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Operation Security

Requirement ATMSP-023-01:

ATM cybersecurity organization shall ensure the coordination of security operations, monitoring and continuous improvement of information processing.

Requirement ATMSP-024-01:

ATM cybersecurity operations shall include IT, OT, IACS and CNS/ATMs infrastructure in the scope of security operations.

Operation Security

Requirement ATMSP-025-01:

ATM cybersecurity operations shall maintain the effectiveness of security measures throughout their lifecycle.

Requirement ATMSP-026-01:

ATM cybersecurity shall be operated from dedicated zones having dedicated physical and logical security perimeter.

Operation Security

Requirement ATMSP-027-01:

ATM cybersecurity shall prevent the exploitation of technical vulnerabilities on IT, OT, IACS and CNS/ATM infrastructure.

Requirement ATMSP-028-01:

ATM cybersecurity shall forbid the use of personal mobile devices for CNS/ATM activities.

Operation Security

Requirement ATMSP-029-01:

ATM cybersecurity shall ensure that professional mobile devices do not constitute an unacceptable risk to security (as per Chapter 7 Risk Management).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cybersecurity Management

Communication Security

- Keep control on connections & connectivity
- Ensure consistency of logical and physical zones (Assets)
- Implement defense in depth based on asset criticality regarding safety and operability

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Communication Security

Requirement ATMSP-030-01:

ATM cybersecurity shall maintain an up to date mapping of networks and their interconnections.

Requirement ATMSP-031-01:

ATM networks shall be logically or physically segregated based on their criticality regarding safety and operability.

Communication Security

Requirement ATMSP-032-01:

ATM cybersecurity shall ensure that wireless technologies and access to the Internet do not constitute an unacceptable risk to safety and security (as per Chapter 7 Risk Management).

In cooperation with

ICAO

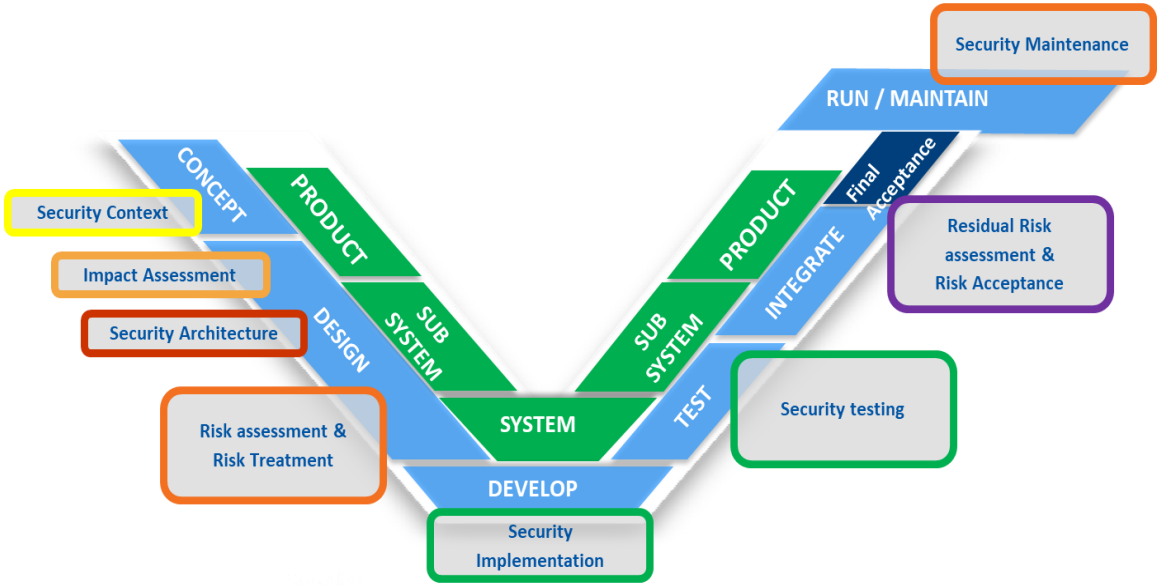
canso
civil air navigation services organisation

AIRBUS

Network segregation

System Acquisition, Development and Maintenance

- Integrate security to development life cycle
- Based on risk management
- And Vulnerability management at any time



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

System Acquisition, Development and Maintenance

Requirement ATMSP-033-01:

ATM cybersecurity shall ensure that information security is an integral part of CNS/ATM information systems throughout the entire lifecycle.

Additional information: This also includes the requirements for information systems which provide ATM services over public networks.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

System Acquisition, Development and Maintenance

Requirement ATMSP-034-01:

ATM cybersecurity shall ensure that CNS/ATM information systems are designed based on the following principles (list not exhaustive):

- No single, nor common point of vulnerability;
- Definition and implementation of security coding rules;
- Vulnerability management on COTS software and hardware;
- Implementation of industry standards and recommendations (NIST, OWASP, …).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

When you development projects….

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Suppliers and Partners (S & P)

- Define your security expectations: S & P security requirements
- Assess S & P's security maturity
- Monitor and follow-up S & P
- Include procurement in security team

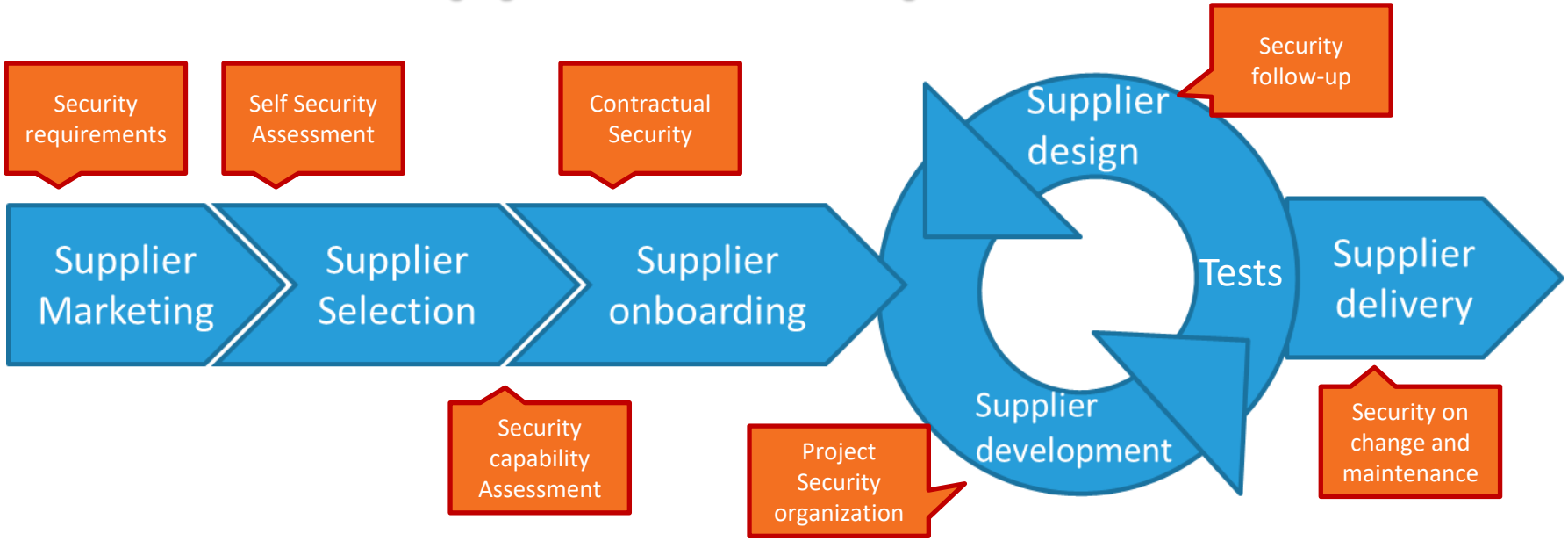
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Suppliers and partners



In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Suppliers and partners

Requirement ATMSP-035-01:

ATM cybersecurity shall provide End-to-End security from supply chain to partners in the scope of CNS/ATM cybersecurity management system.

Requirement ATMSP-036-01:

ATM cybersecurity shall ensure relationships with external entities do not constitute an unacceptable risk (as per Chapter 7 Risk Management).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Talk about suppliers….

In cooperation with

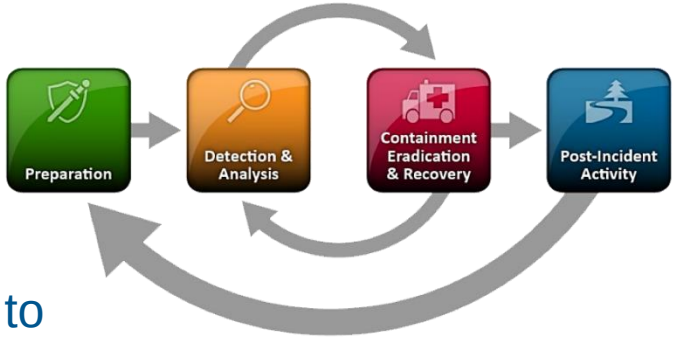
ICAO

canso
civil air navigation services organisation

AIRBUS

Security Incident Management

- Be prepared: by training, regular tests, serious game play, …
- Define communication rules and identify key decision makers (escalation process)
- Connect incident with crisis and Business Continuity Management
- Ensure to collect logs in a consistent way between Security, Safety and Operability (critical asset focused)
- Ensure consistency of incident detection with risks to improve incident accuracy and priority



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Security Incident Management

Requirement ATMSP-037-01:

ATM cybersecurity shall ensure a consistent and effective approach to the management of CNS/ATM security incidents, including communication on security events and weaknesses.

Requirement ATMSP-038-01:

Safety and Business Continuity shall be the main priorities of ATM security incident management.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Cybersecurity incidents and procedures…

Business Continuity

- Identify triggering criteria
  - From Business Continuity to Disaster Recovery
  - From Business Continuity to Crisis
- Reconsider Business Continuity including malicious act and supply chain security
  - Review alternatives sites based on criticality and security
  - Consider security in relocation to alternative business sites
  - Include security in Test of shifting and recovery procedures

Business Continuity

Requirement ATMSP-039-01:

ATM Business continuity shall be designed in accordance with Risk Management outcomes.

Requirement ATMSP-040-01:

ATM cybersecurity shall establish a consistent, effective and common strategy to manage CNS/ATM security and safety through integration of all Stakeholders with common efforts, sharing information, to complete their operational objectives.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Business Continuity Plan (BCP)

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Personal Data

Requirement ATMSP-041-01:

ATM cybersecurity shall ensure the privacy and protection of personally identifiable information in accordance with applicable regulations.

In cooperation with

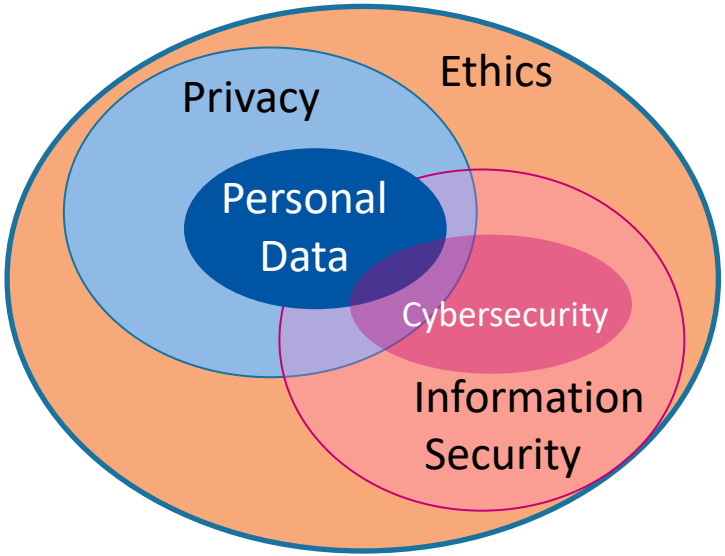
ICAO

canso
civil air navigation services organisation

AIRBUS

Personal Data

- Establish and maintain personal data processing inventory and perform privacy impact assessment
- Nominate the DPO and establish personal data governance (policy and procedures)
- Pay attention to legal aspect of exchange of data with US (Privacy Act) and EU (GPDR)
- Implement minimized data collection and avoid data interconnection
- Check data duration storage and implement data purging



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Compliance

- Perform Third party Security audit and deliver formal statement
- Check compliance to regulation
- Verify consistency of governance and organization
- Evaluate Efficiency of security controls
- Perform Intrusion test
- Support continuous improvement

Regulations

- Law
- External requirements / Standards

Governance & Organization

- Policies
- Processes
- Roles and Responsibilities

Implementation

- Cyber Security: Architecture & Configuration (Best practices)
  - Equipments & softwares
  - Accounts network, ...
- Physical Security: Protection & Detection
  - Physical controls and detection
  - Video Protection and CCTV

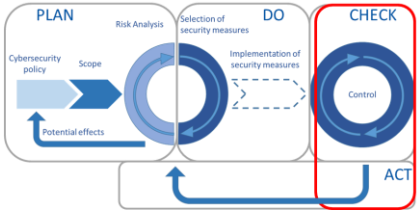
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Compliance

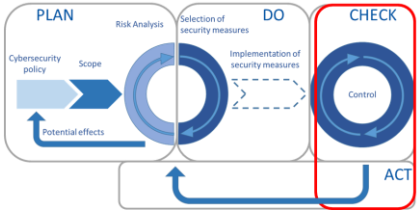


Requirement ATMSP-042-01:

CNS/ATM information systems shall receive recognized security validation qualification before entry into service in compliance with ED 205 Process standard for Air Traffic Management / Air Navigation Services (ATM/ANS) ground systems security aspects of certification / declaration.

Additional information: recognized accreditation process is to be defined at national level and made applicable for critical infrastructures.

Compliance



Requirement ATMSP-043-01:

CNS/ATM information systems security validation shall be controlled on a regular basis.

Requirement ATMSP-044-01:

ATM cybersecurity shall ensure that any deviation, detected through the validation process, does not constitute an unacceptable risk (as per Chapter 7 Risk Management).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

External Requirements …..

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Use Case example
& Cyber security kick off activities

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Agenda

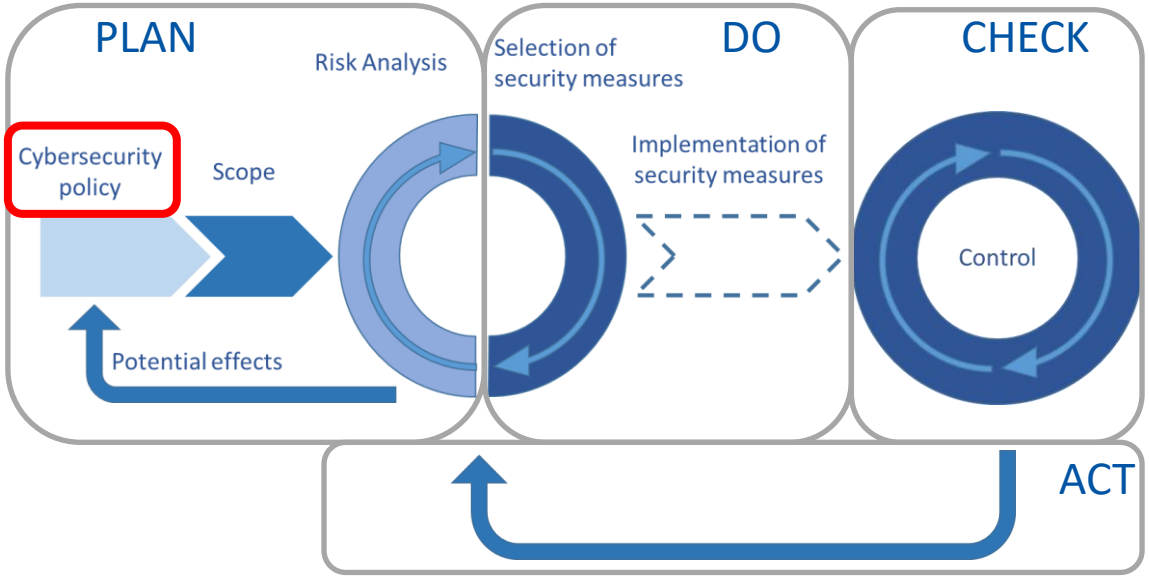
- Start your ATM Security Management System
- Cybersecurity policy commitment
- Expected activities
- Use case example Communication System
  - Description
  - Architecture
  - Functional Impact identification
  - Samples of traceability and justification with the security policy
- Conclusion
- Q&A

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Start your ATM Security Management System

- Customize this cyber security policy to your own context
- Check compliance with regulation
- Make it applicable and communicate



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Cybersecurity policy commitment

- Empower the organization
  - Nominate key people
  - Assign roles and responsibilities
- Lead implementation of ISMS (Top-Down communication)

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Expected activities

- Implement Security baseline, based on standards & best practices (ISO 27002, NIST, IEC 62443) and begin implementation.
- Start working using a process-based method
- Introduce ISMS in organization's processes
- Evaluate risk and make risk mitigation decisions
- Follow-up on risk mitigation implementation until acceptance
- Monitor risks and set up threat intelligence analysis
- Check the effectiveness (Auditing & pen testing)
- Repeat the above

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Use case: Communication System

- The system in charge of all communications between controller and aircraft (voice and data)
- It manages the frequencies and enable the pilots
  - To be aware other aircraft in the same zone
  - Collect and manage route instructions
- Switched from circuit based to software and voice over IP

In cooperation with

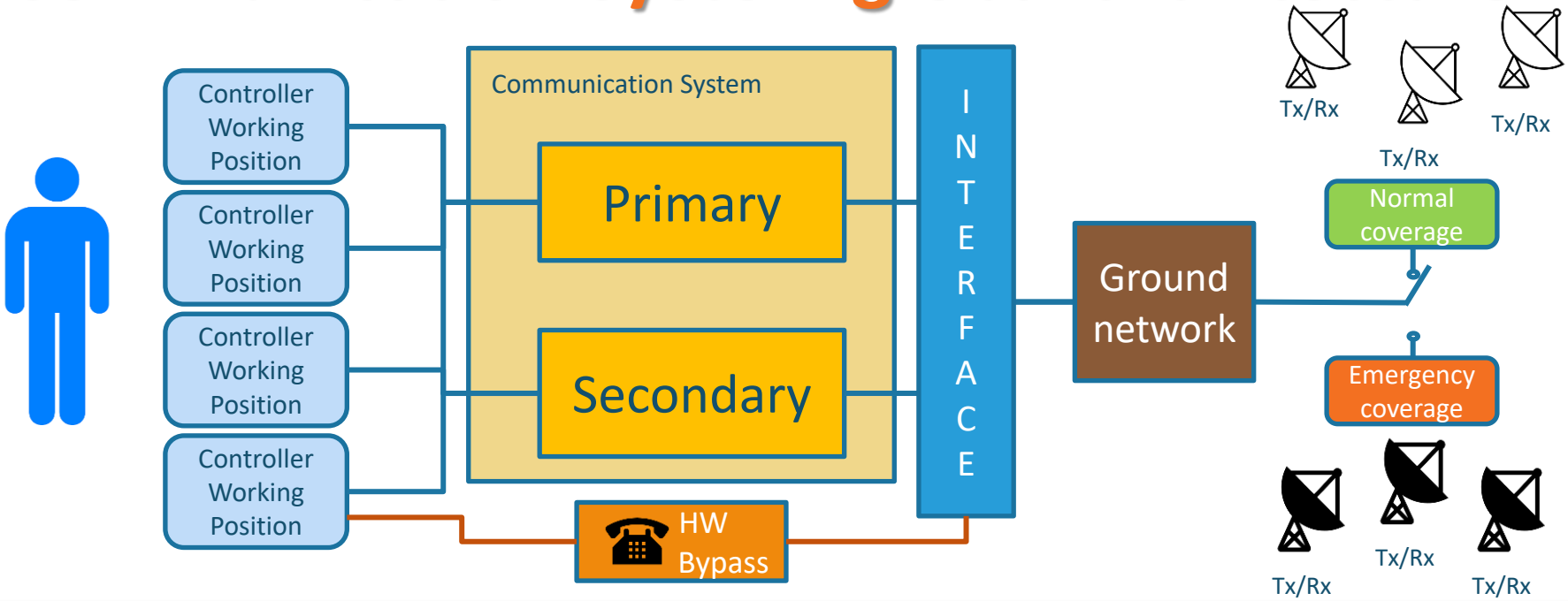
ICAO | canso civil air navigation services organisation | AIRBUS

Cybersecurity functional impact

Consequences evaluation:

Phase	Impact description	Impact Level (Safety)
Ground / Taxi	Loss of data transmission: **controller overload, capacity limitation on Take-off and Landing**	Major to Hazardous
	Loss of communication: Delays, AoG	Minor to Major
Climb / Approach	Loss of communication: Closure of controller position / **ATC Zone closure / « Clear the sky » procedure**	Hazardous to Catastrophic
Cruise	Loss of communication: **High capacity limitation**	Hazardous to Catastrophic

Communication System global architecture



Feared events identification

Staff & Users

Controller Working Position

Controller Working Position

Controller Working Position

Controller Working Position

Communication System

Primary

Secondary

HW Bypass

INTERFACE

Ground network

Normal coverage

Emergency coverage

Tx/Rx

Tx/Rx

Tx/Rx

Tx/Rx

Tx/Rx

Tx/Rx

Staff & users

Requirement ATMSP-012-01:

Personnel shall be part of ATM security during all employment phases:

- Before employment: through measures such as background checks in accordance with local regulations;
- **During employment: by developing a security culture through regular training and raising awareness; and**
- After employment: by ensuring the respect of the de-provisioning process and reminding staff of non-disclosure commitments.

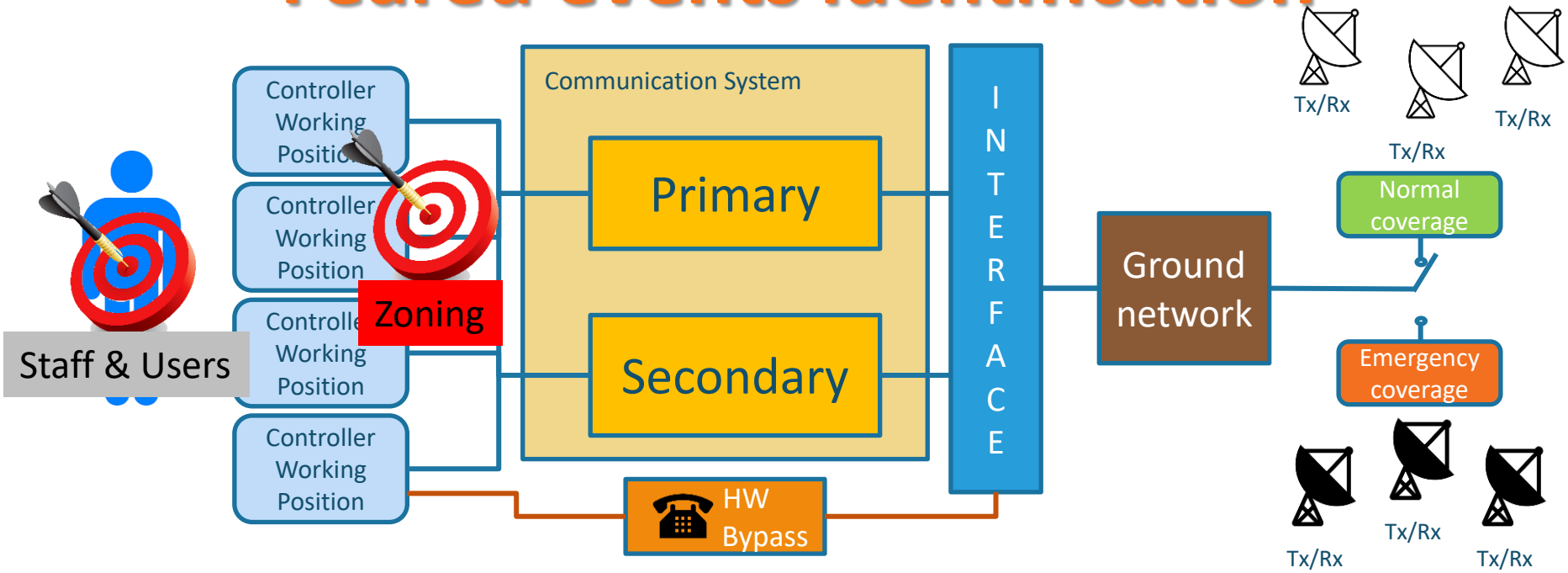
Requirement ATMSP-013-01:

Security personnel shall ensure that individuals with access to ATM facilities, controlled areas and ATM sensitive data do not constitute an unacceptable risk (as per Chapter 7 Risk Management).

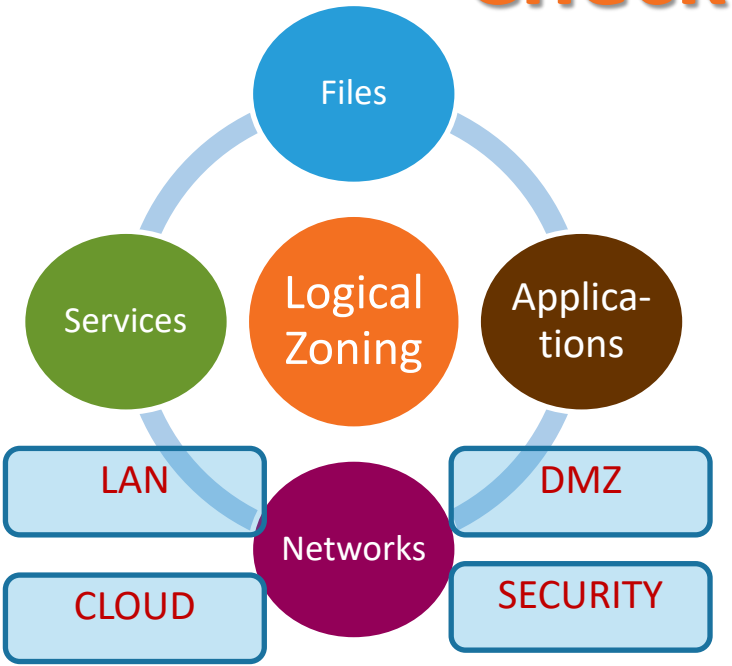
Staff and users

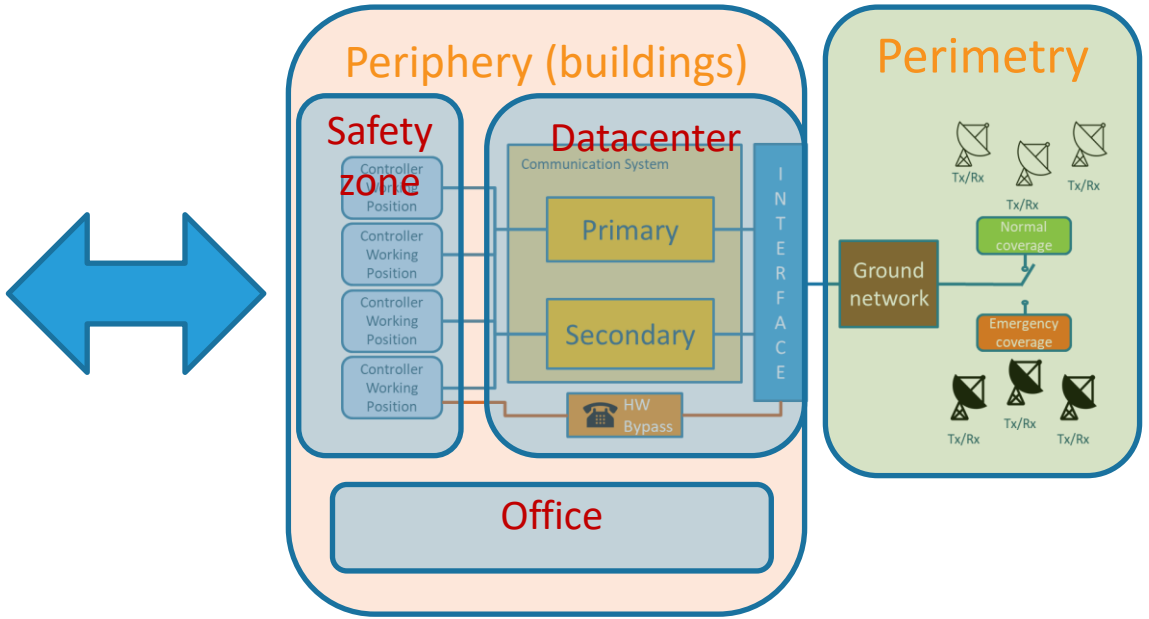
- Extend background checks to all employees including those outside airport zones
- Define cyber security training plan
- Establish connections with authorities
- Implement strict decommissioning of users accounts and rights

Feared events identification



Check zoning consistency





In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Access control & Physical and Environmental Security

Requirement ATMSP-019-01:

ATM physical security shall safeguard IT, OT, IACS and CNS/ATM infrastructure, against unlawful interference and unauthorized access.

Requirement ATMSP-020-01:

ATM physical security shall identify zones hosting CNS/ATM assets according to their criticality regarding safety and operability.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Access control & Physical and Environmental Security

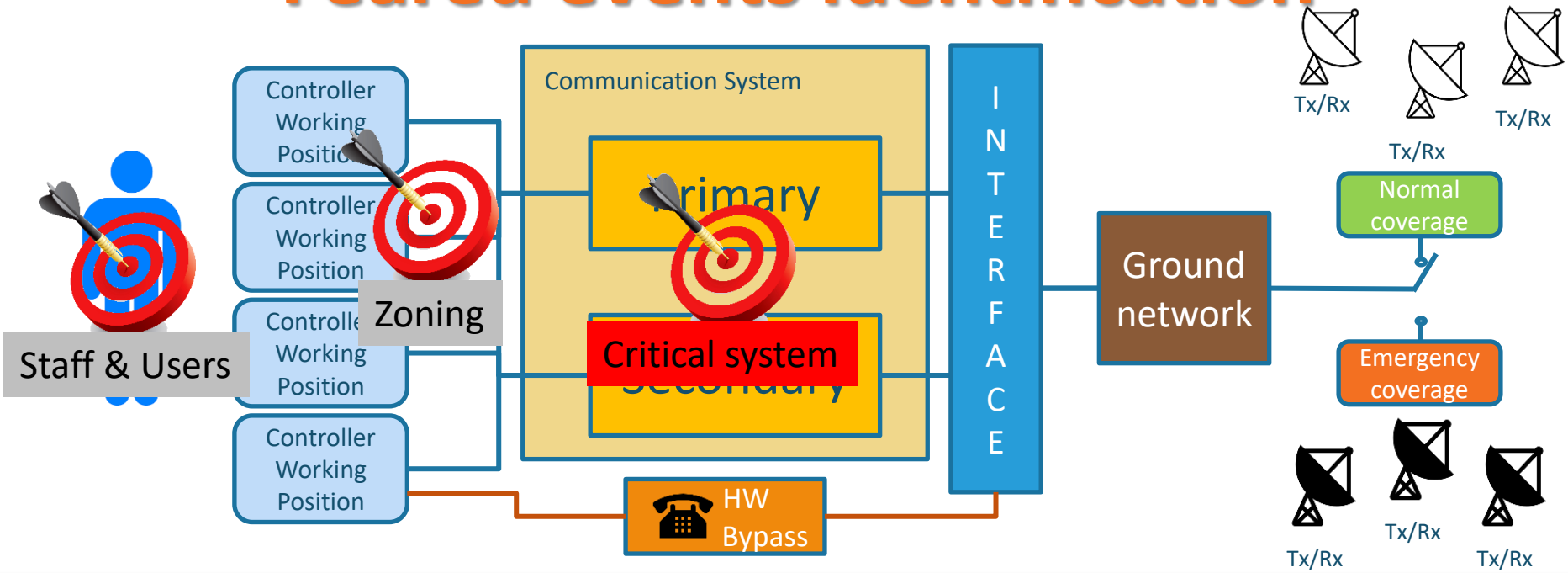
Requirement ATMSP-018-01:

Access to any ATM assets shall be granted on:

The verification of absence of unacceptable risk (as per Chapter 7 Risk Management);

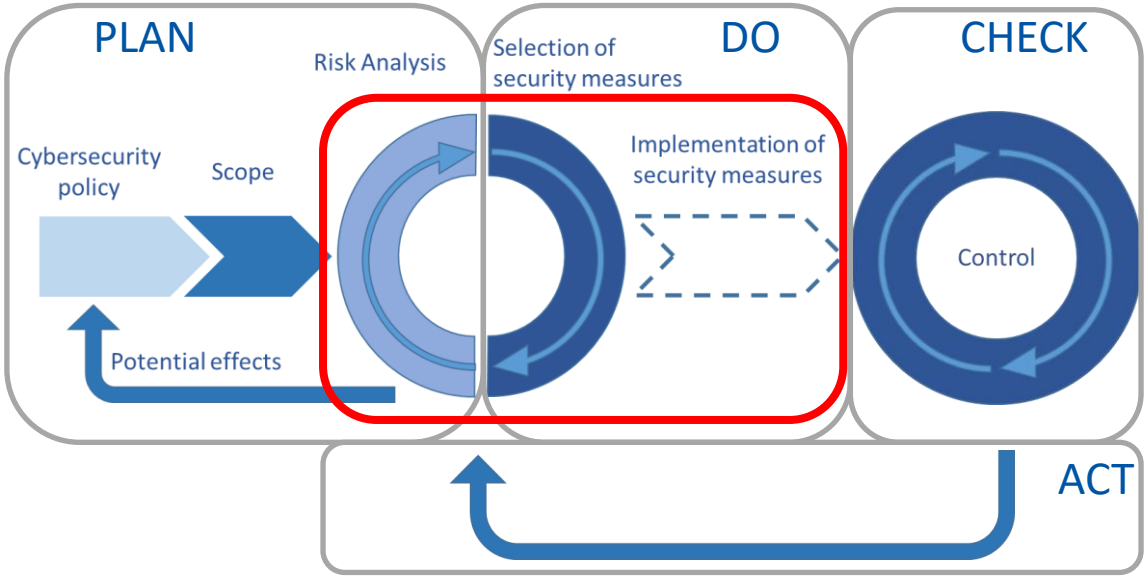
need-to-know basis).

Feared events identification



Manage risks on critical systems

- Implement best security practices (ISO 27002, NIST)
- Identify evaluate & reduce unacceptable risks
- Accept residual risk **ONLY** when mitigation plan is implemented



In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

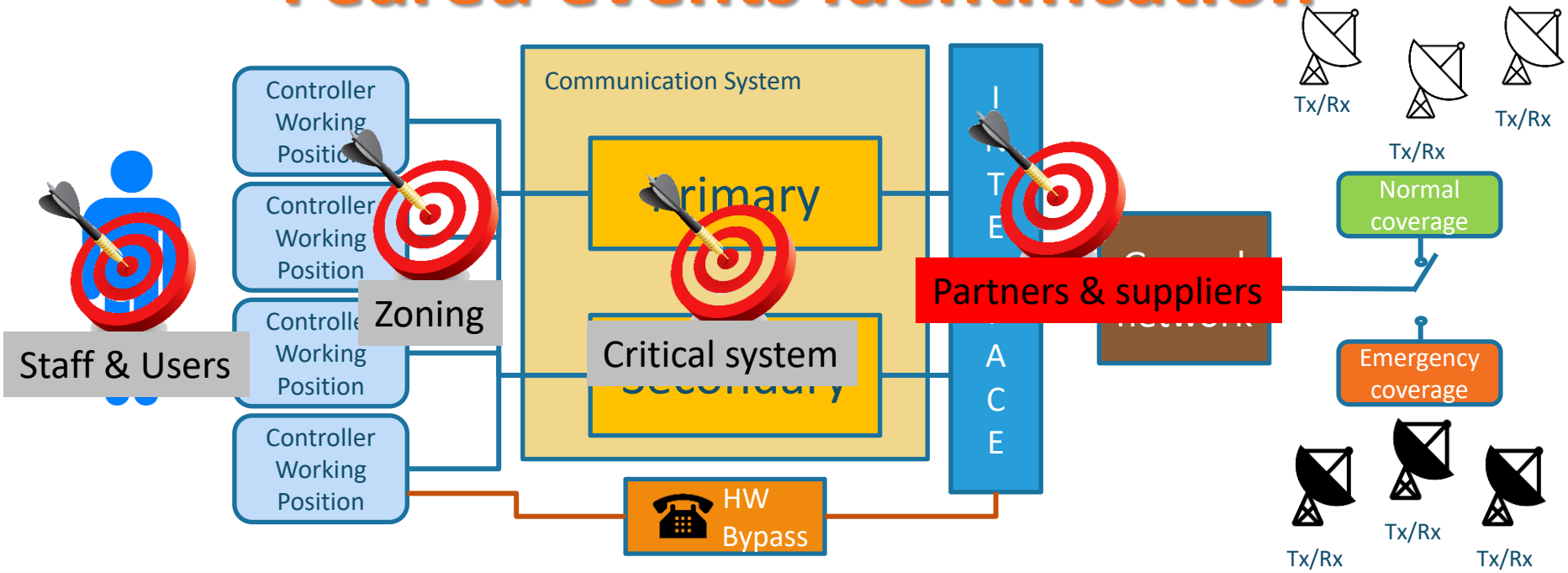
Cyber security Risk Management

Requirement ATMSP-006-01:

ATM Security Risk based approach shall implement technical security measures and operational security measures (policies and processes) to reduce risk to an acceptable level regarding:

- (Intentional) Successful cyber-attack,
- Human error,
- Accident or incident,
- Impact from natural disaster.

Feared events identification



Suppliers and partners

Requirement ATMSP-035-01:

ATM cybersecurity shall provide End-to-End security from supply chain to partners in the scope of CNS/ATM cybersecurity management system.

Requirement ATMSP-036-01:

ATM cybersecurity shall ensure relationships with external entities do not constitute an unacceptable risk (as per Chapter 7 Risk Management).

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Suppliers and partners

- Make sure you integrate **ALL** your suppliers and partners in cyber security risk management process
- Define security objectives to be achieved on project, people, deliverables, interconnections …
- Ensure strict follow-up of security process

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

What do you have?

Conclusion

- **“The supreme art of war is to subdue the enemy without fighting”** Sun Tzu – The art of war
- Manage risks and put in place security controls to deter and prevent cyberattacks
- Be prepared to react in case cyber security risk materializes:
  - Business continuity plan
  - Incident & crisis management

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Thanks for your attention

Q&A

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

MONTRÉAL
(HEADQUARTERS)

PARIS
(EUROPEAN AND
NORTH ATLANTIC)

BEIJING
(ASIA-PACIFIC
SUB-OFFICE)

CAIRO
(MIDDLE EAST)

MEXICO CITY
(NORTH AMERICA AND CARIBBEAN)

DAKAR
(WESTERN AFRICA)

BANGKOK
(ASIA-PACIFIC)

NAIROBI
(EASTERN AFRICA)

LIMA
(SOUTH AMERICA)

THANK YOU!