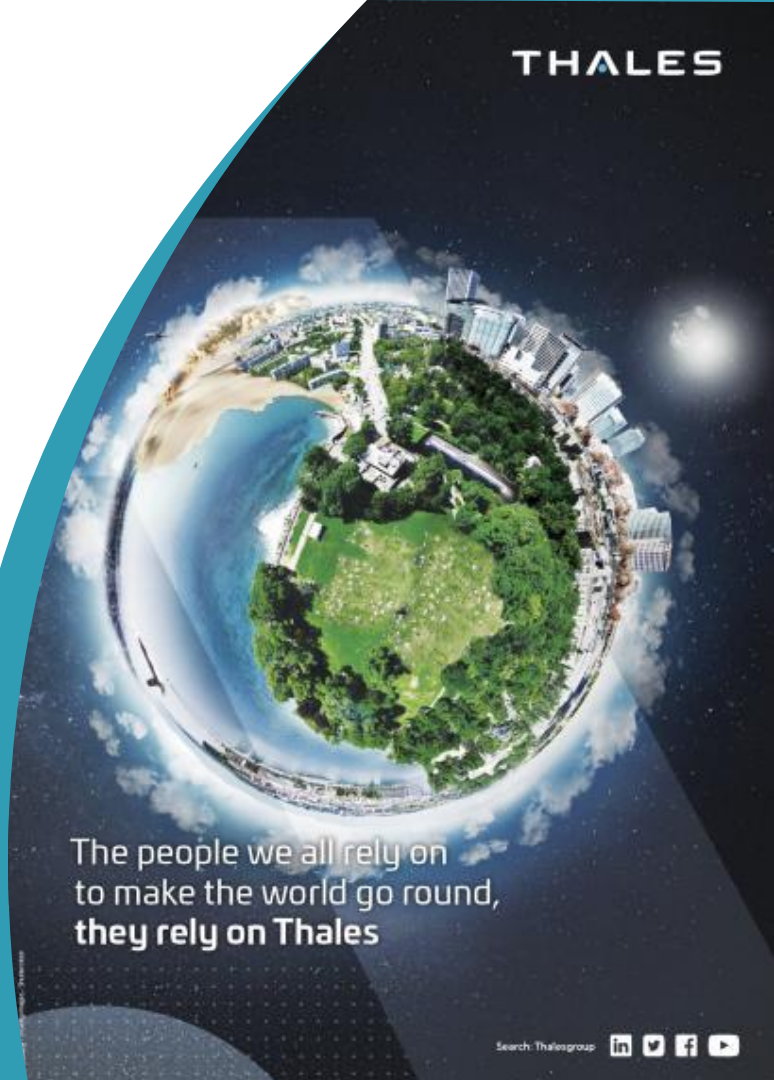
THALES

Cyber-Security for Air Traffic Management

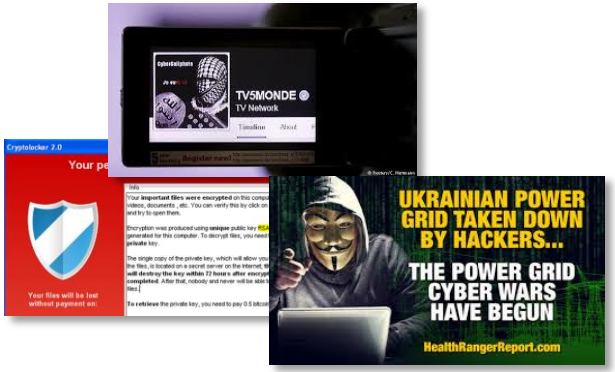
ICAO

Mexico November 2018



Cyber-Attacks are multiplying

- Ransomware attack blacks out screens at UK Airport
- Hackers deface Airport screens in Iran with anti-government messages
- FBI Warns of cyber-thieves targeting Aviation
- Cyber-chaos at Heathrow
- Access to airport's security system sold on dark web
- Ransomware targets Civil Aviation Authorities, ...
- ....

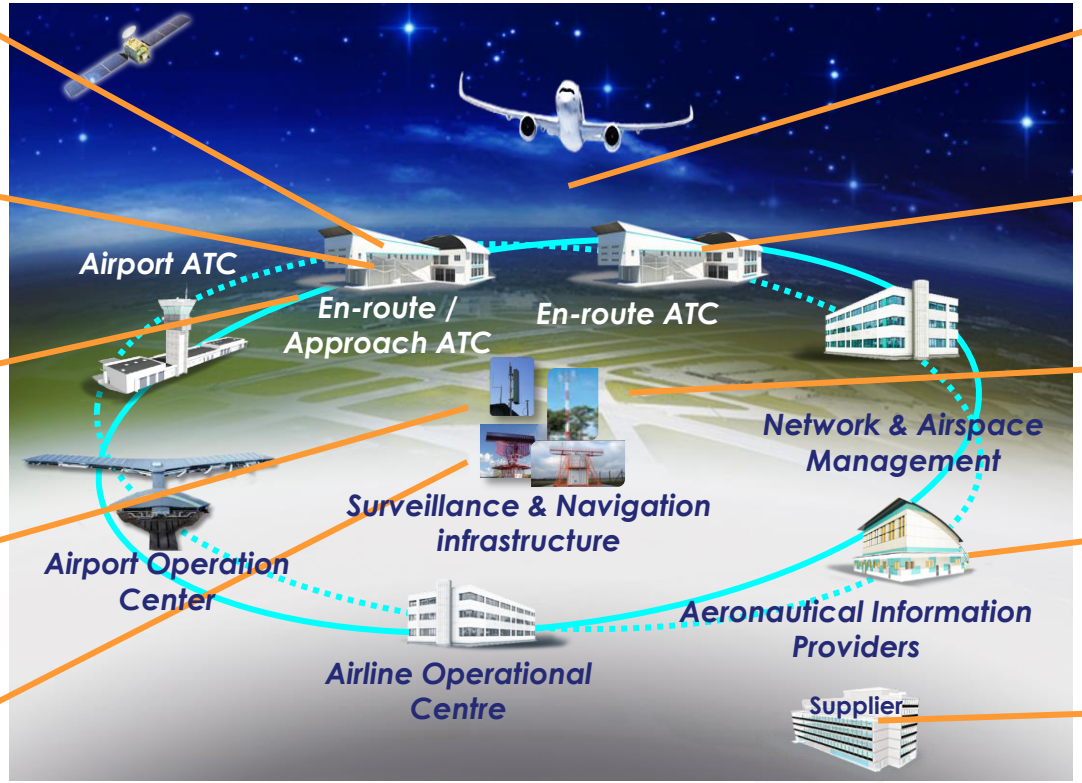


In 2016 more than 60 new ransomwares appeared (Source SANS)

THALES

Some feared events for ATC among many others !

- Insertion of infected USB key on Online ATC system
- Login usurpation on ATC system technical position
- Remote intrusion in ATC LAN
- Spoofing of ADS-B radio signal
- Spoofing of radar data over interconnection network



- Controller or Pilot usurpation over Datalink
- Malware injection in maintenance
- Spoofing of GPS time
- Denial of Service on Aeronautical Information server
- Malware injection in supply chain

THALES

Some common vulnerabilities in ATM

Technical

- Lack of (strong) authentication on many critical data flows (surveillance, aeronautical data, data link, ..)
- Weak integrity control on many critical data flows
- Lack of knowledge on configuration and highly exposed/exploitable vulnerabilities
- Limited detection of tentative of intrusion on critical networks
- Often no malware detection (off-line or on-line)
- Isolation between the security domains often questionable
- …

Procedural

- Weak vulnerability management and understanding of underlying risks
- Limited procedure (Safety can help) to maintain minimum service continuity in case of cybersecurity breach
- ….

Other

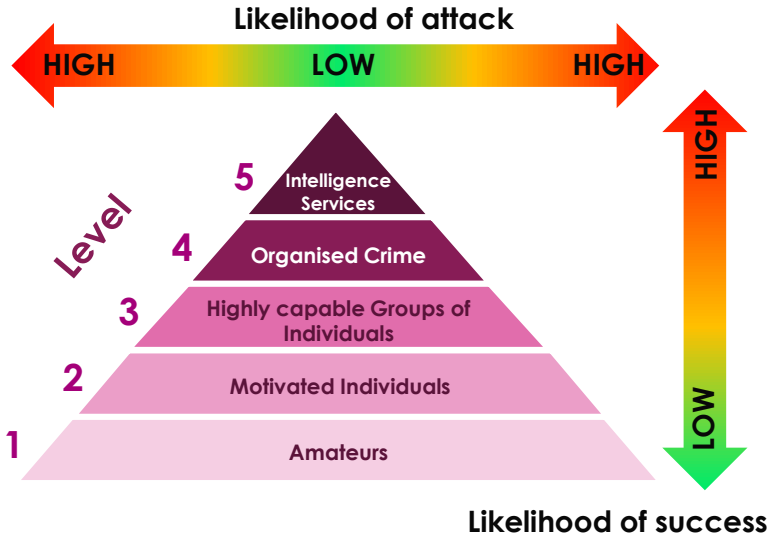
- Cyber-security policy and organizational measures underestimated
- …

THALES

Cyber-Threat is Insider/Outsider including very intentional acts

- **Insider Threat** including inadvertent actions which involves individuals with access to organizations' systems continues to hold top place with **roughly 55 %** of the attacks
- **Outsider threat** is responsible for roughly 45 % of the attacks

- **Untargeted attacks** continue to be **most common** and widespread malicious actions
- **Targeted attacks** which hints very intentional acts and sophistication are **often against State's Critical Infrastructure Operators** : ANSP classification in many Countries



THALES

ATM is more and more exposed to Cyber-threat

THREAT IS INCREASING

- Number and sophistication of attacks
- Hacking tools increasingly accessible
- Most legacy ATM data communication protocols & RF signals not secure-by-design

AND ATTACK SURFACE IS GROWING

- Standard COTS components for interoperability
- More automation
- Connectivity/CDM/SWIM and Digital Transformation

More preparedness required

The ATM Digital Transformation has already started

THALES

THALES response to make the ATM Cyber space safe and highly available

THALES

Thales expertise in Cybersecurity

OPERATION AND CYBERSECURITY OF CRITICAL INFORMATION SYSTEMS FOR OVER **130** CUSTOMERS

HIGH-GRADE SECURITY PRODUCTS AND SOLUTIONS (CONFIDENTIAL OR TOP SECRET) FOR **50** COUNTRIES INCL. NATO COUNTRIES

PROTECTION OF THE WORLD'S BANKING TRANSACTIONS **80%**

SECURITY FOR **19** OF THE **20** LARGEST BANKS

CYBERSECURITY FOR **9** OF THE TOP **10** INTERNET GIANTS

2,000 CYBERSECURITY SPECIALISTS

5 CYBERSECURITY OPERATIONS CENTRES

5 DATA CENTRES

amadeus

GALILEO

THALES OneSKY THE FUTURE OF AIR TRAFFIC MANAGEMENT

EUROCONTROL

malaysia airlines

AIRFRANCE KLM

Department for Transport

ARMÉE DE L'AIR

AIR CANADA

DGA

AIRBUS DEFENCE & SPACE

AIRCARAÏBES

THALES

THALES combines Cyber Security & ATM domain Expertise

CYBERSECURITY OPERATION CENTRES (CSOC)

CYBER CONSULTING & TRAINING TEAMS

HIGH GRADE CYBERSECURITY COMPETENCE CENTRES

HIGHLY SECURED DATACENTRES

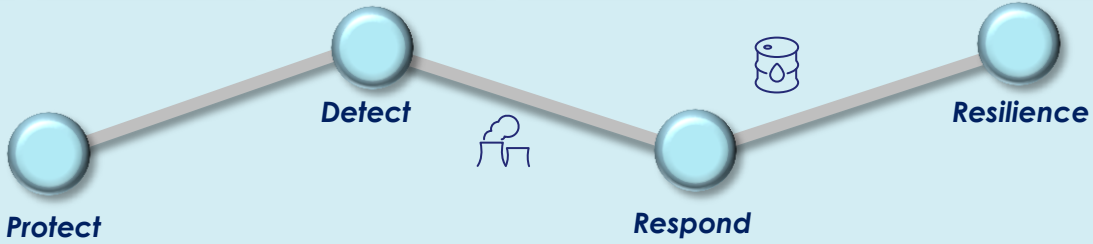
COMPUTER EMERGENCY RESPONSE TEAM

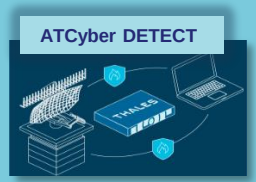
DATA SECURITY HUBS

CyberSecurity for Critical Operators

THALES Expertise

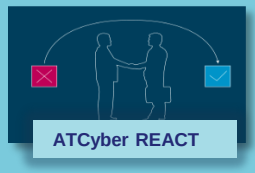
ATM Mission & Architecture





Cyber-Resilience

ATM dedicated CyberSecurity Solutions



Business Continuity Platform

THALES

On-going strong ATM CyberSecurity initiatives supported by THALES

TRUST FRAMEWORK development

- Policy
- Governance
- Measures

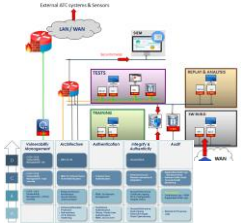
CYBER-RESILIENCE Building

- Awareness, Information Sharing, Analysis Center & sectorial Threat intelligence
- CyberSecurity culture and Training
- Business continuity platform & CONOPS

MINIMUM CYBER-PROTECTION and means of compliance

- Cyber-secure-by design / Upgrades for systems in operation
- New Standard / Evolution
- Certification process, Governance / Authorities

Solutions & Services dedicated to ATM mission & business

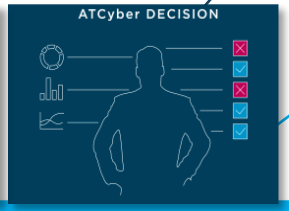


Cyber-Safe ATM
Architecture & Components
Civil/Military Gateways

Trusted Sensors
ATM dedicated Cyber-Agents

ATCC Cyber-Supervision System

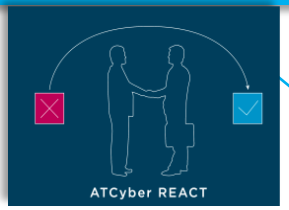
Continuous Vulnerability Management



CyberSecurity Operations Center

FROM PROTECTION **ATCyber** TO RESILIENCE

On-site Cyber-Assessment



Support to Cyber-Crisis Management

Support to Risk Assessment

Cyber-threat Management learning
Immersive Training

SERVICES

THALES

Focus on Cyber-Assessment

- **A proven 5-Step analysis used by Thales for Critical Systems and aligned to ICAO recommendations**

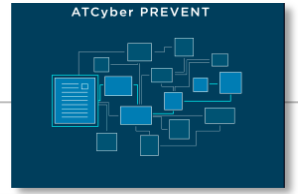
- **Scoping / feared events Workshop with the ANSP**
- **Cyber-Tests and Reviews**
  - On-site Cyber-Security test (non intrusive for systems in operation)
  - Architecture, policy & organizational reviews

- **ANSP's contextual Automation or ATSU Cyber-Exposure assessment**
- **Analysis of the discovered weaknesses & vulnerabilities**
- **Prioritized Cyber-Roadmap & recommended measures for operations**

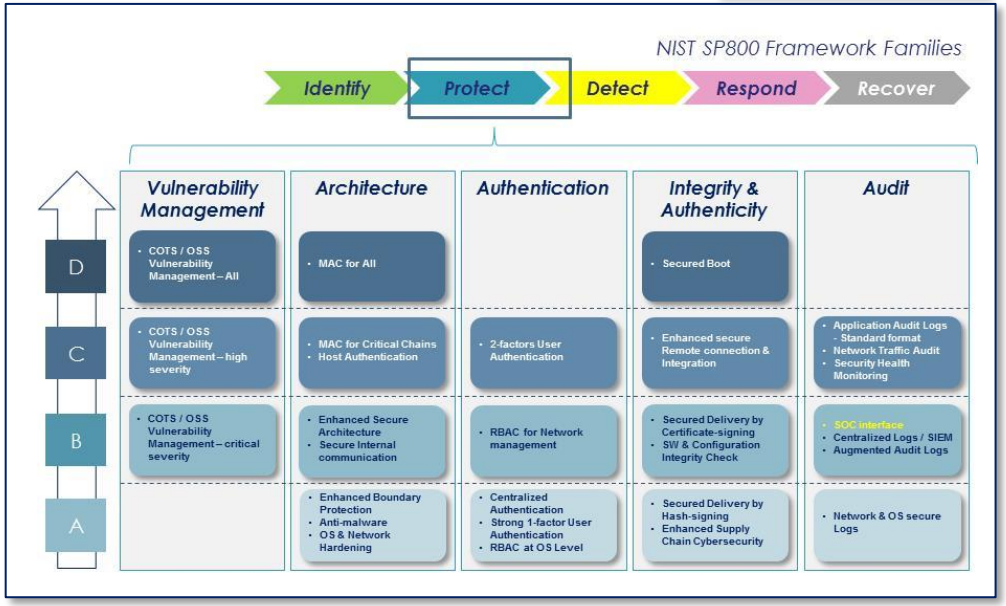
Our Value: Knowledge of cyber-attack paths in ATM for smart analysis

THALES

Focus on TopSky-ATC Cyber-Protection



- Layered approach
- Based on cyber-risk assessment and ICAO, EASA & NIST frameworks
- In-depth protection including ATM specificities and Safety
- Adaptable and scalable according to risk profile at stake



4 layers

- A: OS/Network Hardening
- B : Architecture hardening
- C: Applications hardening
- D: Premium protection

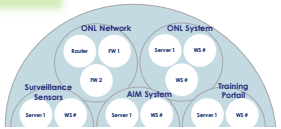
Available for first fit or as upgrades

THALES

Continuous Vulnerability Management Service

ATCyber PREVENT

CyberSecurity Model including key & safety critical assets



ANSP

- Quarterly reports
- Alerting notifications when severity >8
- Remediation recommendation

BUILD

RUN

ATM-CERT

CERTs

COTS supplier

Other sources

Media

Operated by THALES

CERTIST THALES Threat Intelligence

- vulnerabilities notifications
- generic severities
- corrections available (patches)

- Severity scoring - 0 to 10 based on the Cyber-Security Model

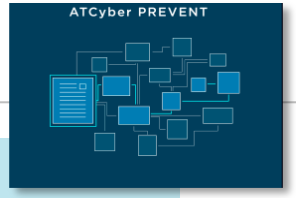
- Consolidated awareness on vulnerabilities
- Filtering according to the CyberSecurity Model

- Remediation analysis for rich CyberSecurity Models e.g. TopSky Systems

Risk characterization according to CVSSv3			
Base score	Temporal score	Environmental score	Criticality
5.3	4.6	8.3	High + (8 > 9)

THALES

Vulnerability Management Process in RUN PHASE



On-site support for high priority remediation

Remediation implementation

ANSP

Priority management on remediation

Operational risk analysis taking into account ANSP's environment

Support to operational risk analysis

Continuous Process

Cyber-Reviews

- Vulnerability watch
- Contextual severity scoring
- Remediation analysis by patching or reduction of attack surface
- Impact of remediation including requalification in particular for Automation Systems

- *Regular vulnerability reports*
- *Alerting notifications*

Cybersecurity is a "state to be maintained"
Our value: Smart qualification of vulnerabilities for ATM domain

THALES

Learning & Training

Awareness sessions

- ATM cyber threat landscape & common attacks
- International regulation and legislation
- Conducting Risk analysis for ATM & ATC Systems
- Cyber-threat management principles & operational center

E-learning

- Best practices in operation & maintenance

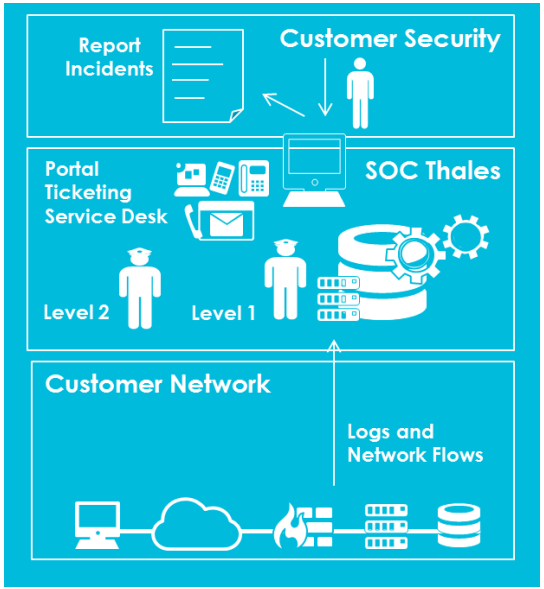
Exercise with immersive training

CYBERLab

Our Value: Make you learn how to respond to cyber-attacks in ATM at no risk before you face them

THALES

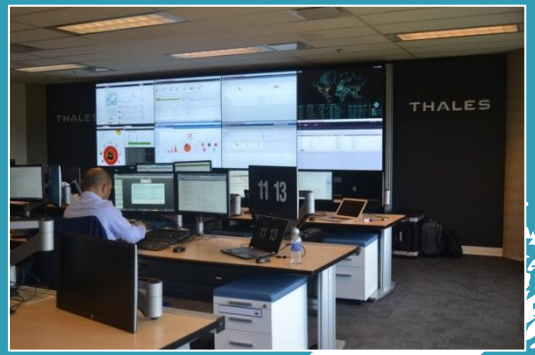
Cybersecurity Operation Center (CSOC)

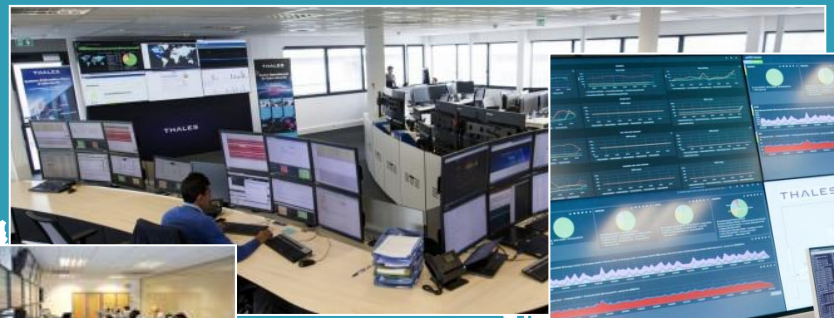


Our Value: Build resiliency

Supervise / anticipate and better stop cyber-attack escalation

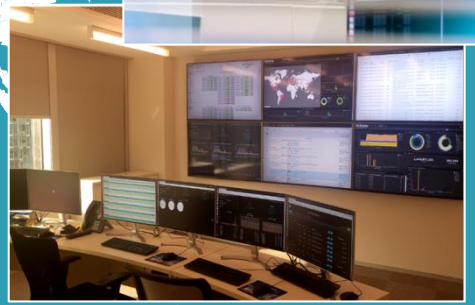

Front-Offi
Hypervisor
Correlation
Analysis
Log
anagement / SIEM
ck-Office
Collection
Firewall
Customer Portal
CSOC
Threat Intelligenc
CISO
CSIRT / CERT
Internal Firewall
Internet Firewall
Servers
Probe/Proxy
Customer In
astructure
IT Operations
INTERNET


THALES


THALES

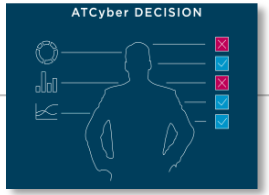

THALES


THALES

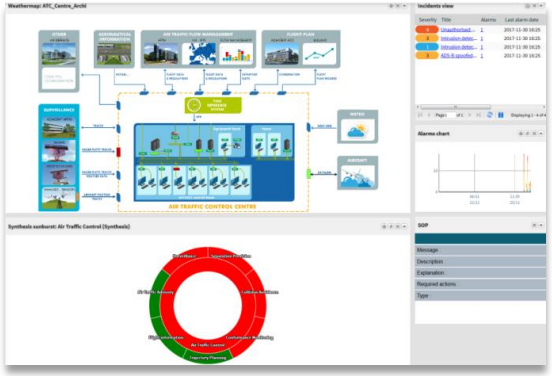



THALES
THALES
Cybersecurity Operations Centre

CNS/ATC Systems Cyber-Supervision CYBELS



- **Synthetic and dynamic dashboard to visualise the impact of cyber-events or incident on ATC services**
- **Based on a dynamic risk analysis & model**
- **Enables to better**
  - Anticipate and stop cyber-attack escalation
  - Take the right decision to minimize impact on critical services for improved Resilience



Thales Cybels-Decision

THALES

Beyond cyber-protection with resilience in operations

Protection

Protecting equipment versus infrastructure/assets
End to end approach to design comprehensive cyber solution covering ATM system but also surveillance, sensors and NAVAIDs

Cyber raises new modes of failures
Safety methodology to be enriched with cyber expertise to set achievable compromise

Legacy protocols are not robust enough
We need improved standards and governance with cyber protection perspective

Your infrastructure is unique your weakness also
You need a dedicated analysis of gaps using a state of the art methodology

Resilience

Cyber security is not your core business
Thales CSOCs provide cybersecurity surveillance monitoring and appropriate measure to isolate the problem and continue operations safely

Improve the resilience of the operations in case of an attack or a failure
Thales solution and methodology support operators to be better prepared to face an attack, to isolate it, to continue operations, and to repair

Secured-by-design throughout the entire project lifecycle
threat and risk assessment shall be continuously updated

THALES

Let us accelerate together now

Thales has the depth and breath to be a trusted partner for ATM CyberSecurity

THANK YOU

THALES