Brazilian Air Force

Department of Air Space Control

Brazilian Air Space Control and Cyber-Security Management

Actual Scenario and Challenges for Future

ICAO - Workshop on Cyber-Security in the ANS

August/September 2022

Presentation Agenda

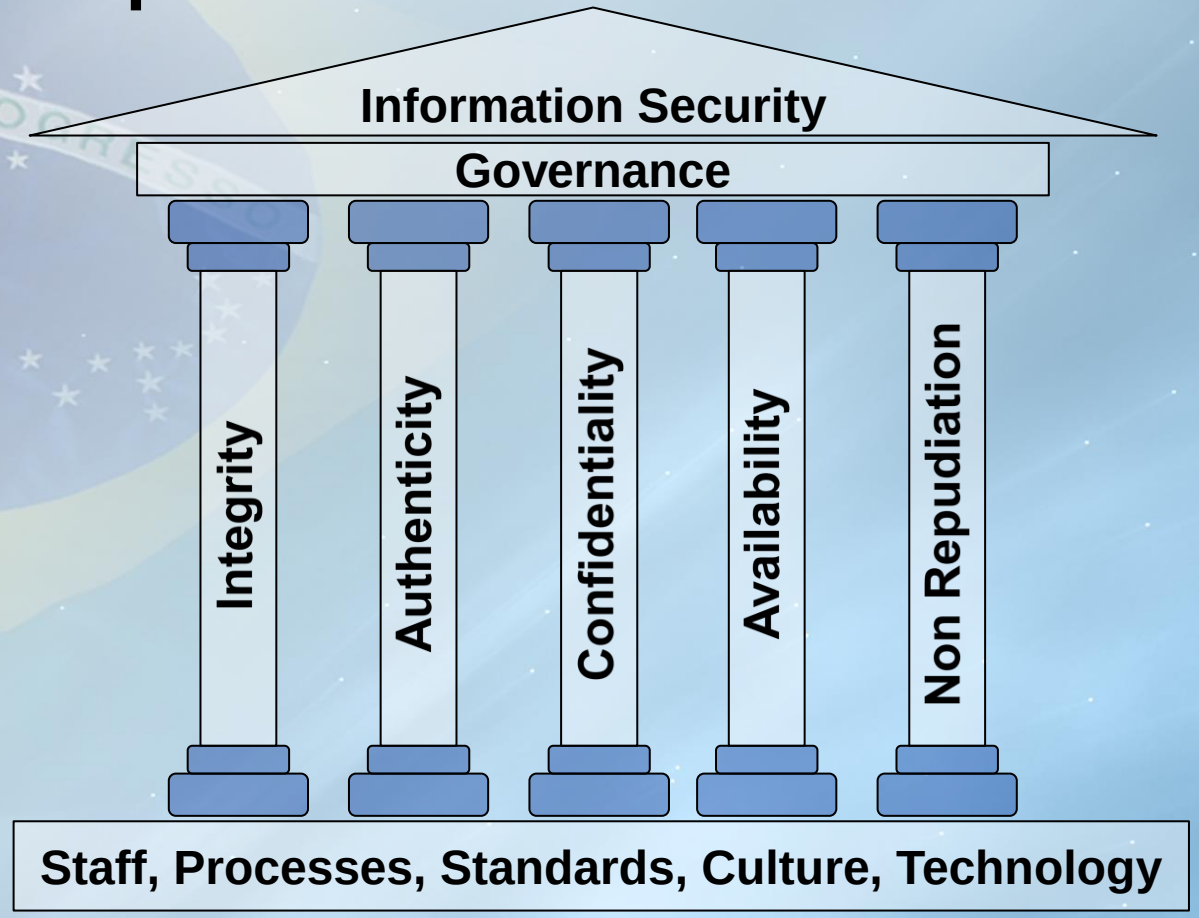
1. Pillars of Information Security & Air Space Control;
2. Technological Evolution;
3. Actual Scenario;
4. Challenges for the Future.

Presentation Agenda

1. Pillars of Information Security & Air Space Control;
2. Technological Evolution;
3. Actual Scenario;
4. Challenges for the Future.

Pillars of Information Security & Air Space Control

Airspace Control is based on information and communication !!!



Presentation Agenda

1. Pillars of Information Security & Air Space Control;
2. Technological Evolution;
3. Actual Scenario;
4. Challenges for the Future.

Technological Evolution

- Analog technology;
- Independent systems;
- Physically limited access.

(jamming, power suply problems, physical attack)

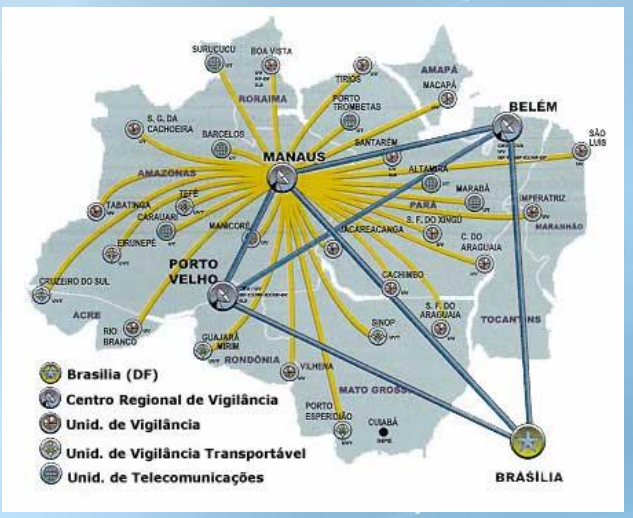
good & easy times...

Technological Evolution

- VoIP;
- Infrastructure evolution;
- Satellite communication.

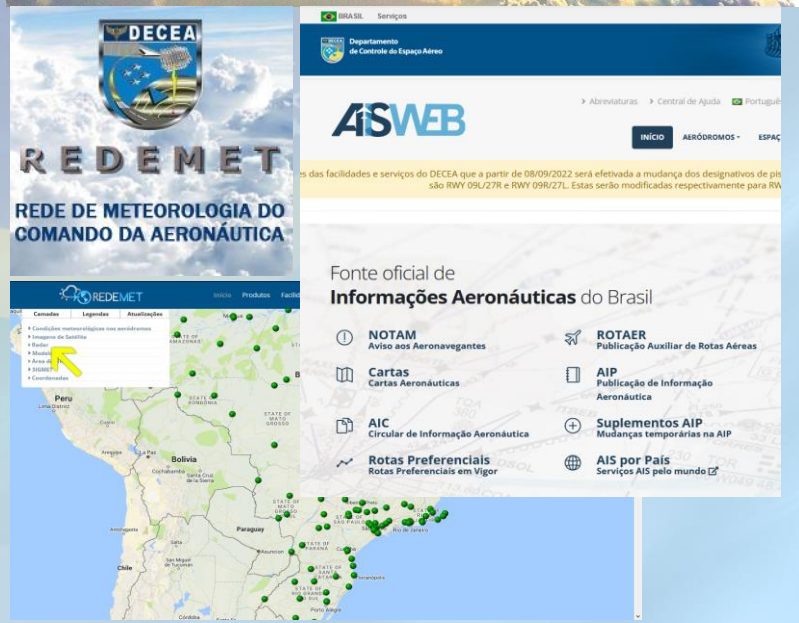
(virus, radio frequency interference)

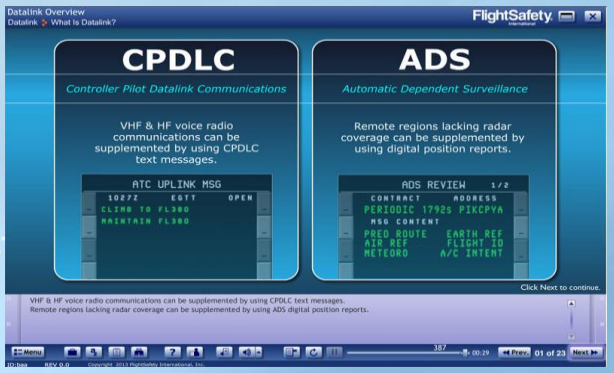
New technologies... still good & easy



Technological Evolution

- **Pilot and flight controller digital communication;**
- **Flight real time data sent for analysis and monitoring (ACARS);**
- **Online weather data (REDEMET);**
- **Aeronautical Information available on the Internet (AISWEB).**



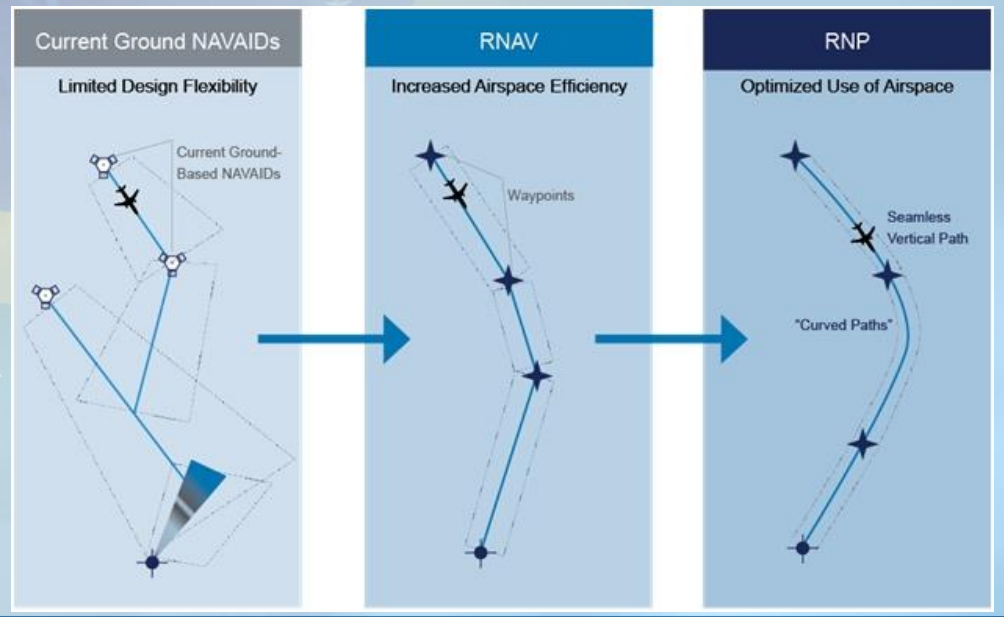


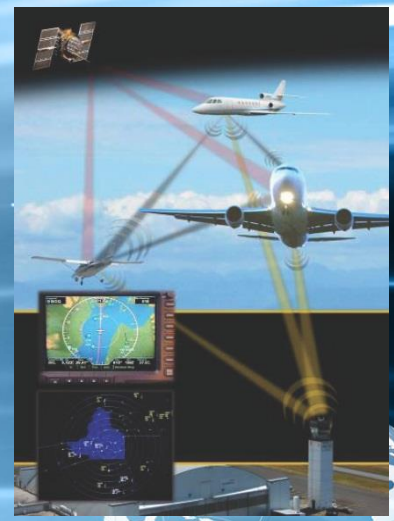
Technological Evolution

- **Performance based navigation (PBN);**
- **Air Traffic Flow Management System (ATFM);**

Greater efficiency in ATM, but Increasing the dependence on digital information and technology!

Also a big increase of attack surfaces !



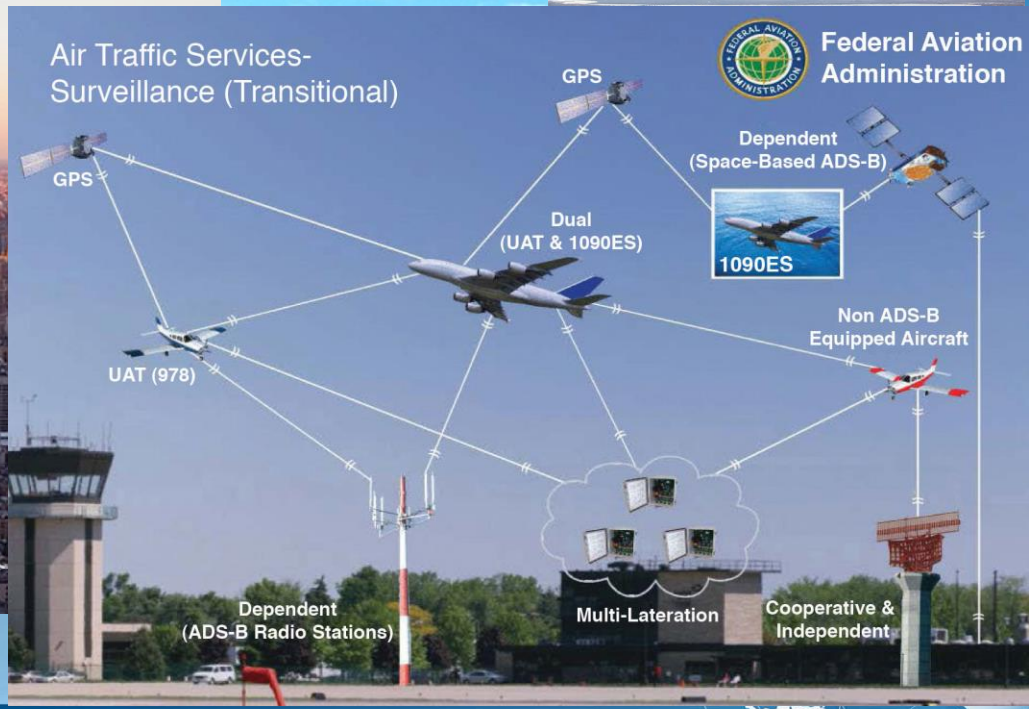


Technological Evolution

We are invited to exercise creativity...

More air space density and automation !

Dependency!



Presentation Agenda

1. Pillars of Information Security & Air Space Control;
2. Technological Evolution;
3. Actual Scenario;
4. Challenges for the Future.

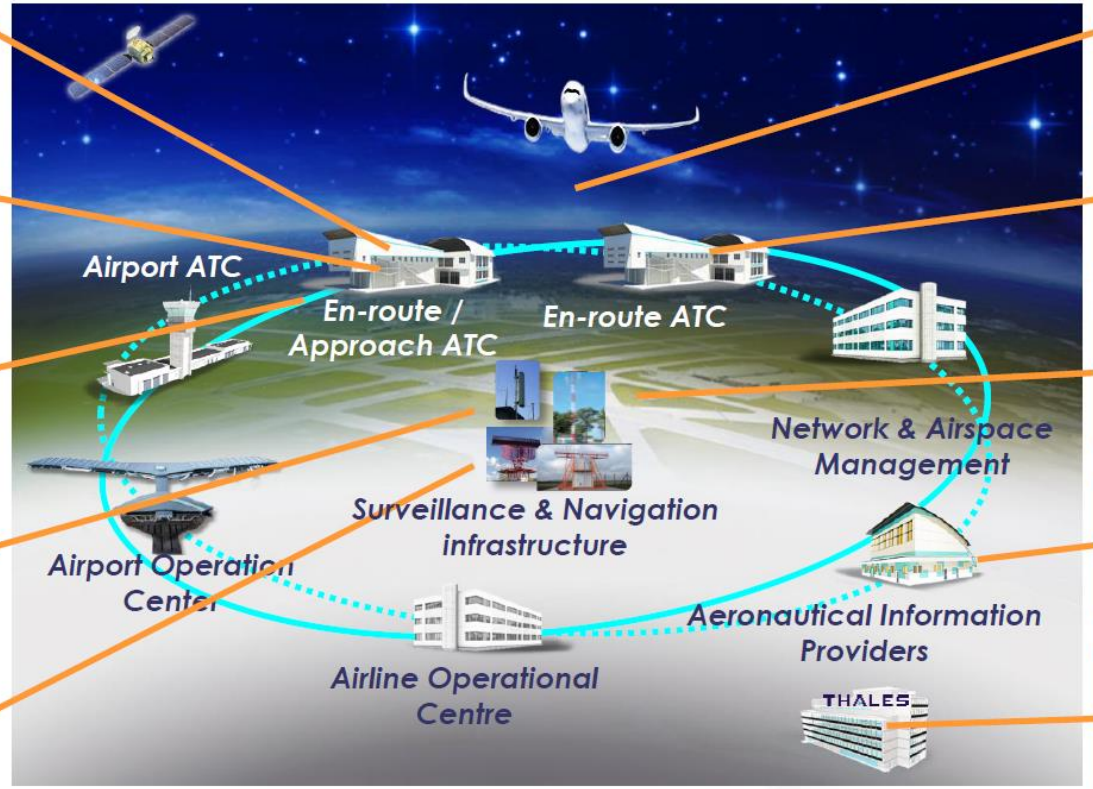
Actual Scenario

Potential Malicious acts against ATM

Many attack surfaces…

Dealing with it each day!

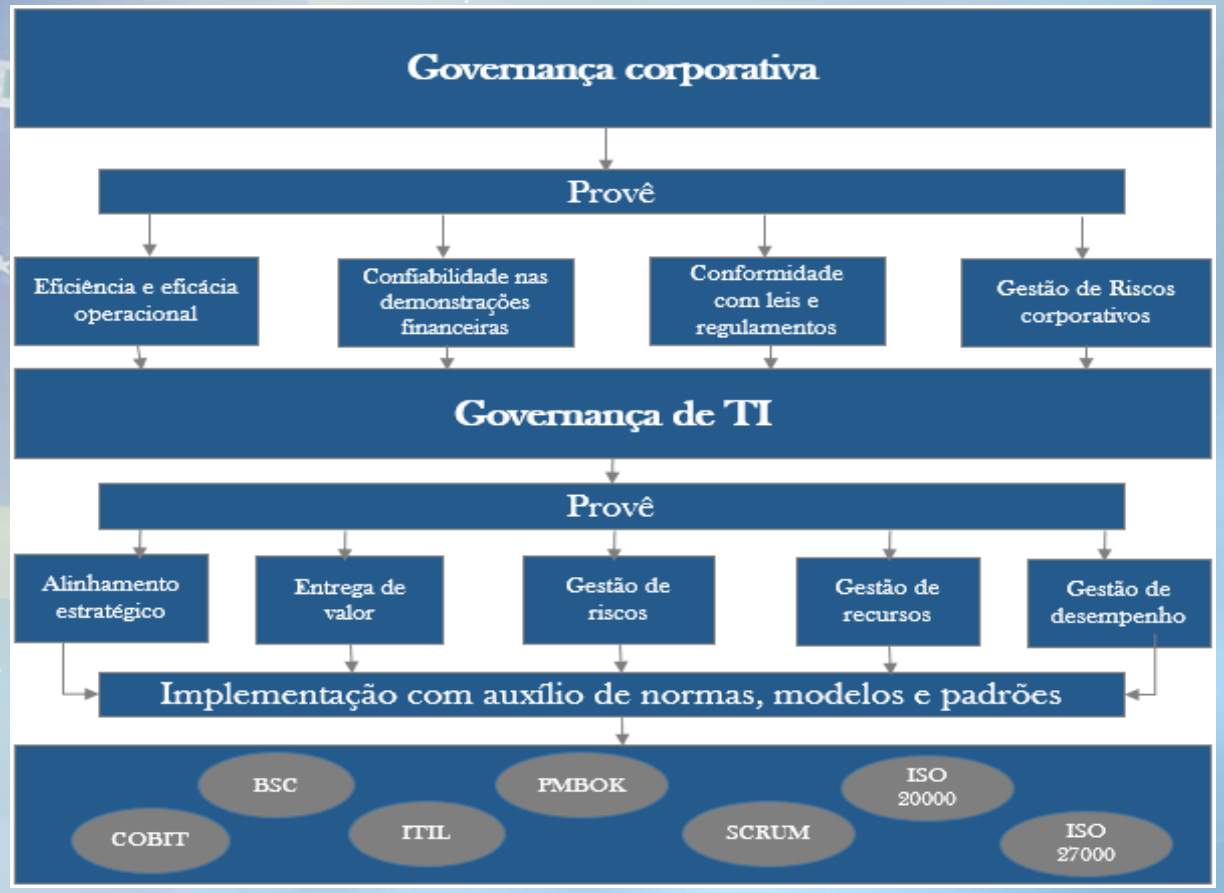
- Insertion of malware infected USB key on Online ATC system
- Login usurpation on ATC system technical position
- Remote intrusion in ATC system Local Area network (LAN)
- Spoofing of ADS-B radio signal
- Spoofing of radar data over interconnection network

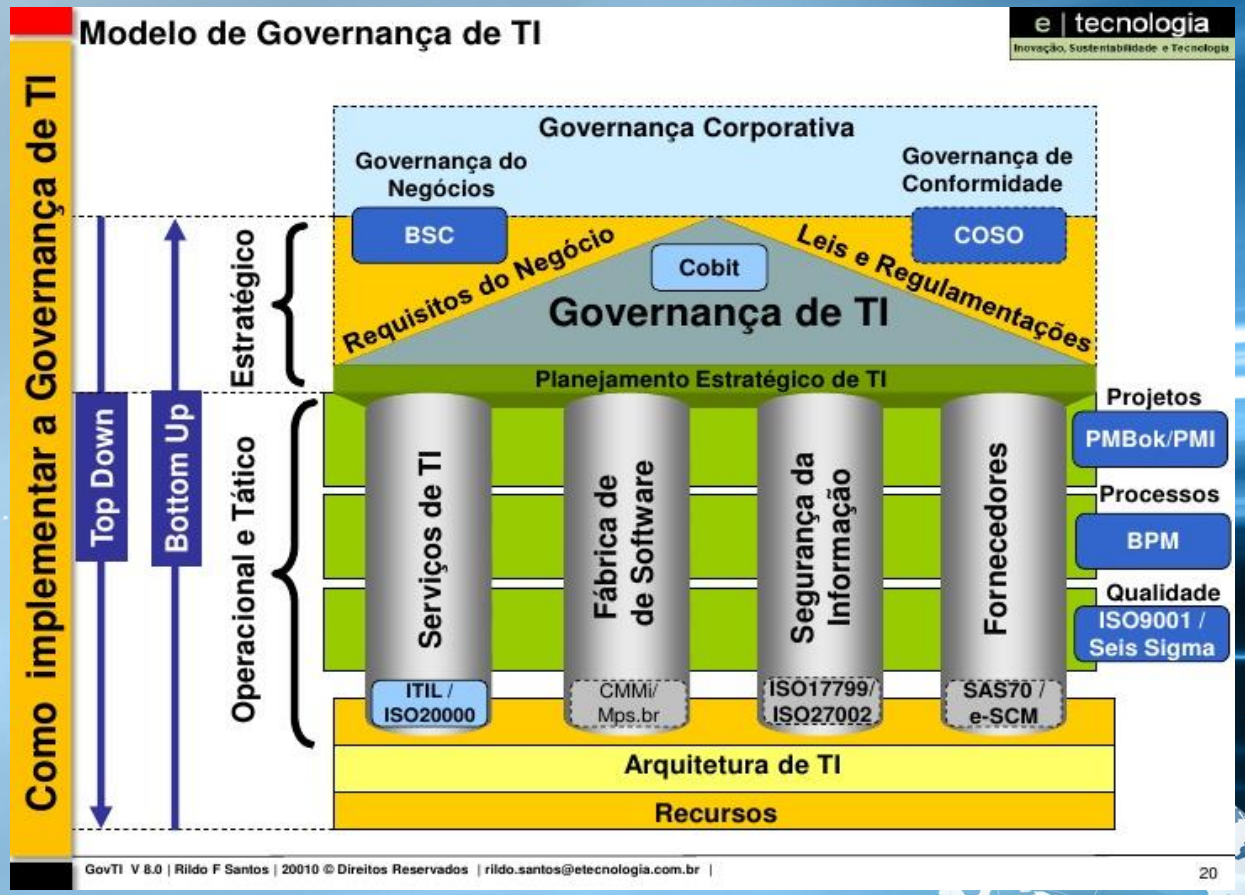


- Controller or Pilot usurpation over Datalink
- Malware injection during maintenance
- Spoofing of GPS time
- Denial of Service on Aeronautical Information server
- Malware injection in software supply chain

Actual Scenario

Applying regulations, standards and best practices.





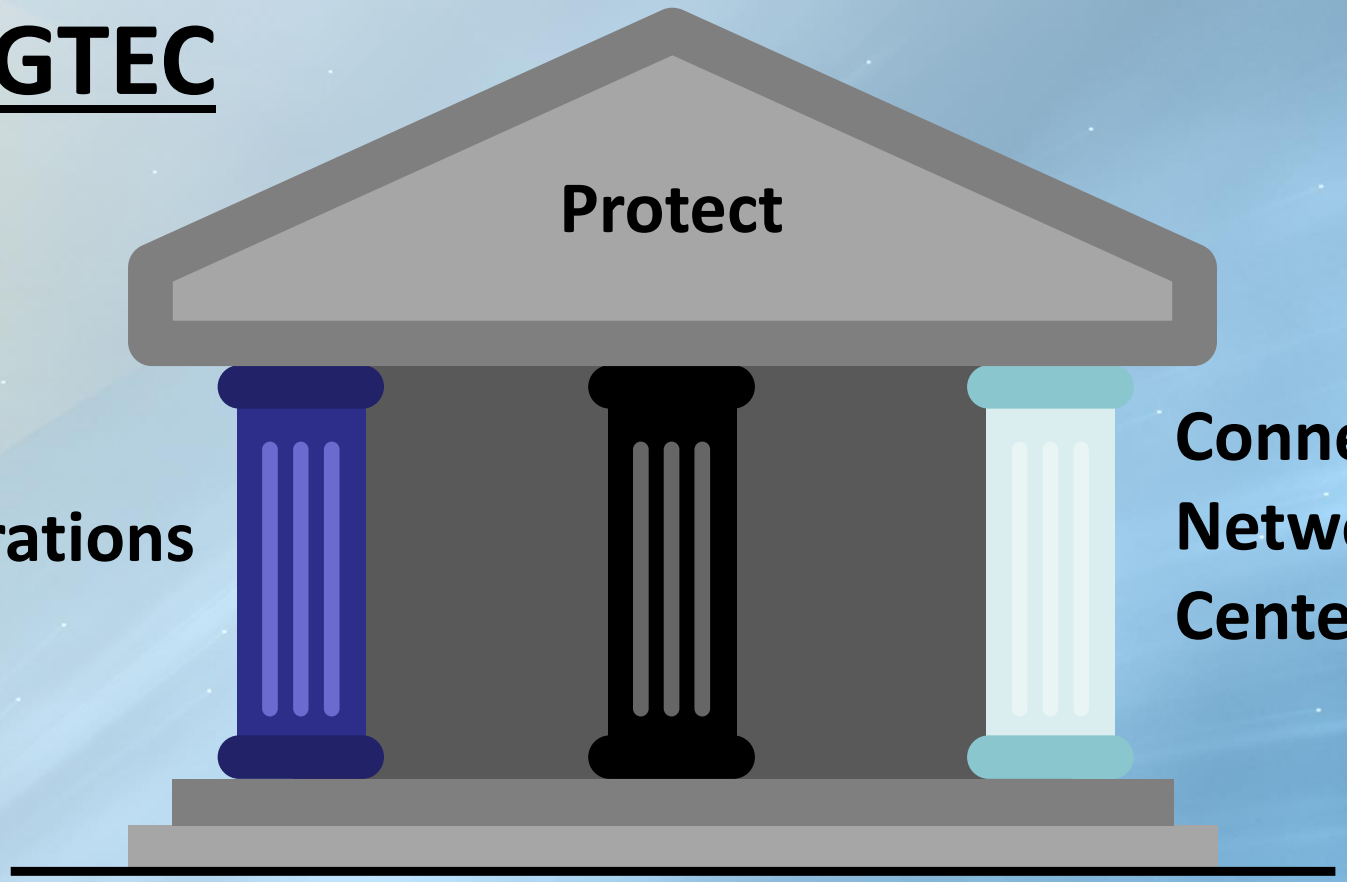
Actual Scenario

CGTEC

DECEA has implemented the Technical Management Center, wich is able to centralize network data communication monitoring, and coordinate corrective actions nationally.

Actual Scenario

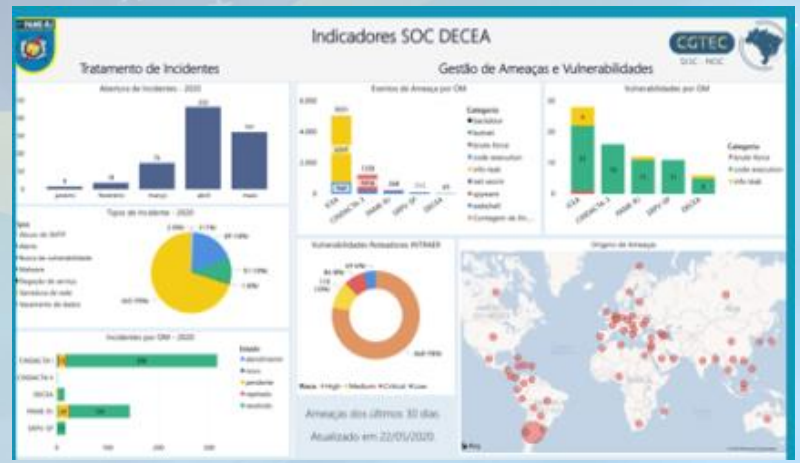
CGTEC

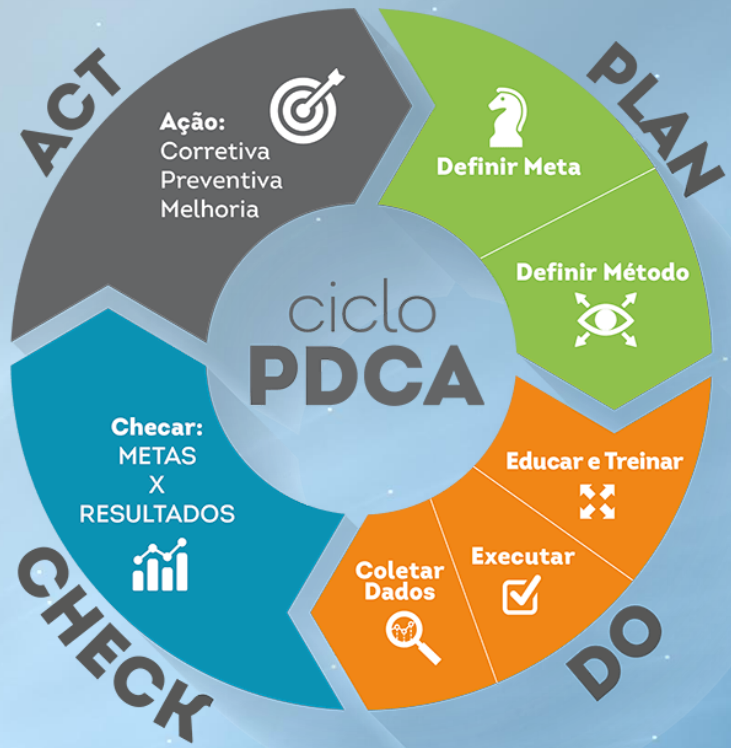


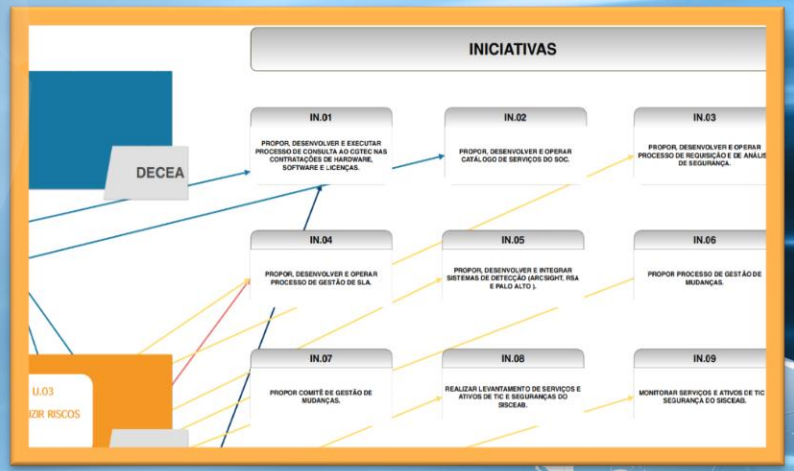
Monitoring…
Security Operations Center (SOC)

Connecting…
Network Operations Center (NOC)

Actual Scenario



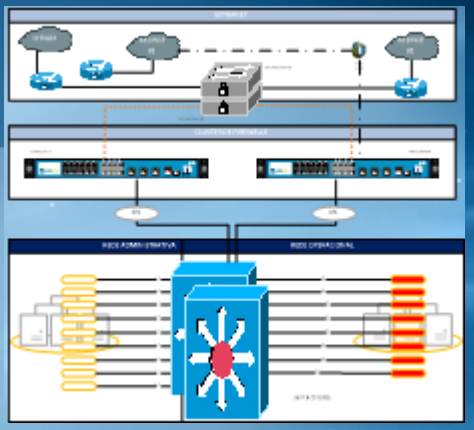




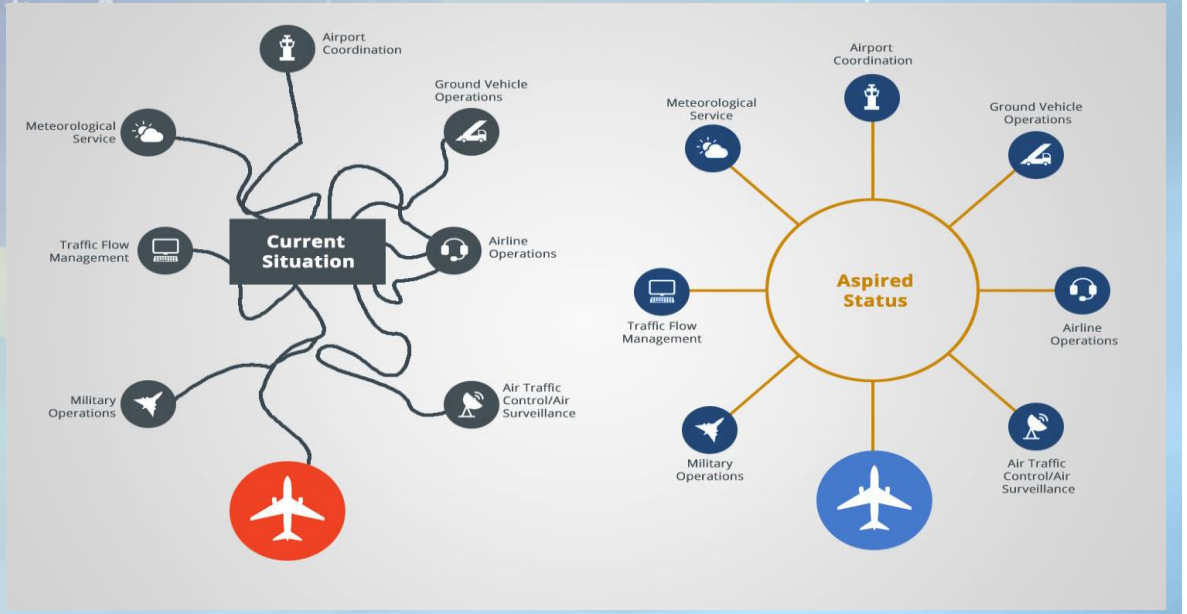
Presentation Agenda

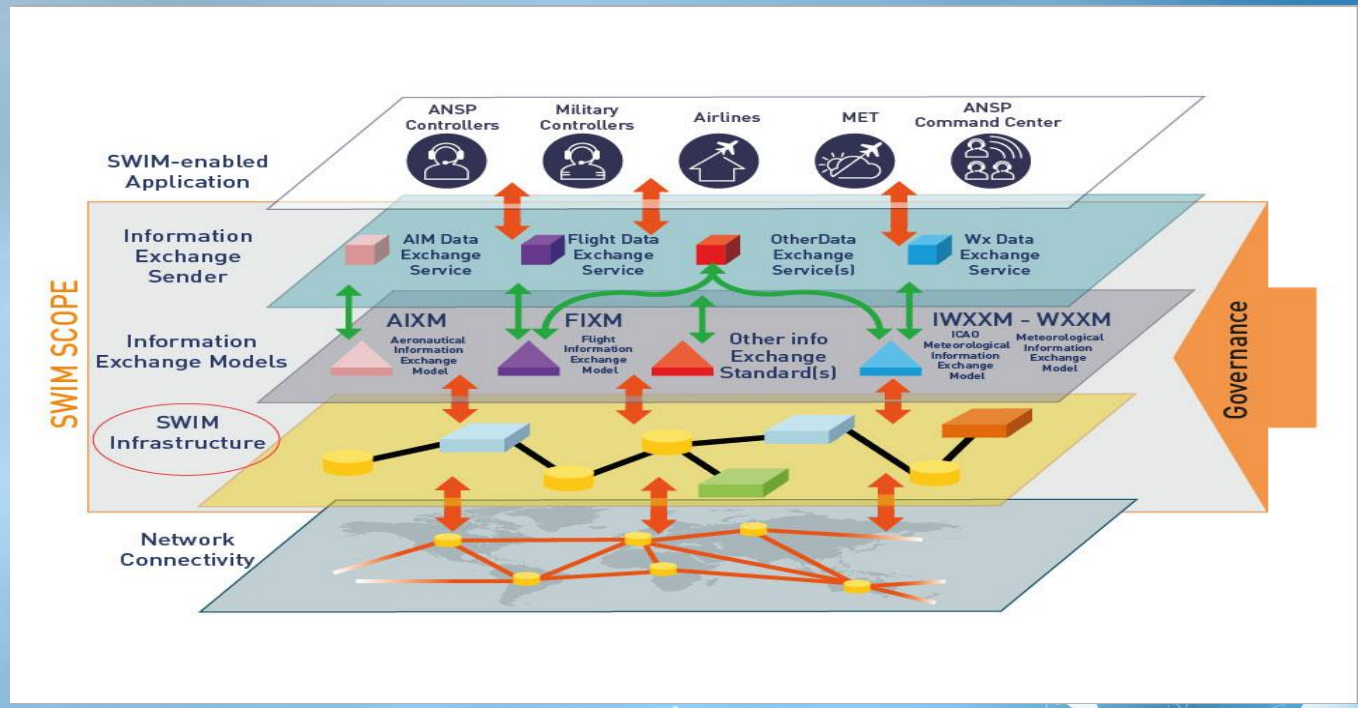
1. Pillars of Information Security & Air Space Control;
2. Technological Evolution;
3. Actual Scenario;
4. Challenges for the Future.

Chalenges for the Future



- Apply High Availability across the entire ATM infrastructure;
- Apply network segregation and defense in depth;
- Simplify and standardize infrastructure and services;
- Prepare services for SWIM approach.





Thanks for you time !!!!

Questions are welcome!