Cyber vulnerabilities in the aviation ecosystem: reducing the attack surface through an international aviation trust framework

Summary

Now, at the beginning of the 21st century, the aviation system is well developed, however, the community is at similar juncture as the beginning of the 2oth century, only this time the civil aviation system itself is being rapidly transformed by a wave of digital technologies that hold great promise but could also expose the aviation system to new threats.

Certain aspects of the digital transformation of the aviation system, based on network connectivity, must be guided to ensure that it generates ever higher-levels of global interoperability and safety. To address this challenge, it is necessary to go back to fundamental principles. It is necessary to establish a system of identity and trust that integrates the wisdom of the Chicago Convention into the digital world that is already overtaking the aviation industry.

Service providers, aircraft manufactures, and avionic producers, are all putting in place their own systems of identity and trust as a matter of necessity. That means, in the near future, an aircraft may need different digital certificates to connect with its satellite communications service provider, retrieve data from the airline operations centre, update its avionics software, download engines monitoring data and other functions. The potential number of proprietary secure links is nearly endless. This patchwork of disparate efforts to reduce the attack surface to air and ground operations will add complexity to the system that will be costly to maintain and will offer a myriad of gaps for adversaries to exploit.

In the absence of global direction, different manufactures and different States will take different approaches. However, if a globally acceptable system for identity and trust that can be used by manned and unmanned aircraft indistinctively as well as by different service providers and users is available it would likely be embraced by many or all.

As such, based on the new vulnerabilities brought by the evolution of the air navigation system through the intense use of digital and connected technologies, the object of this research relates to the vulnerabilities of the aviation system to a cyber-attack and the objective of this thesis is to propose a concept of operations that allows the implementation of a framework able to provide positive digital identification of all members of the aviation community through specific processes and procedures and a virtual network able to preserve the confidentiality, integrity and availability of the data and information being exchanged at the same time it increases the resilience of operations.

Keywords

Attack, digital, identity, interoperability, networks, safety, trust, vulneralities.
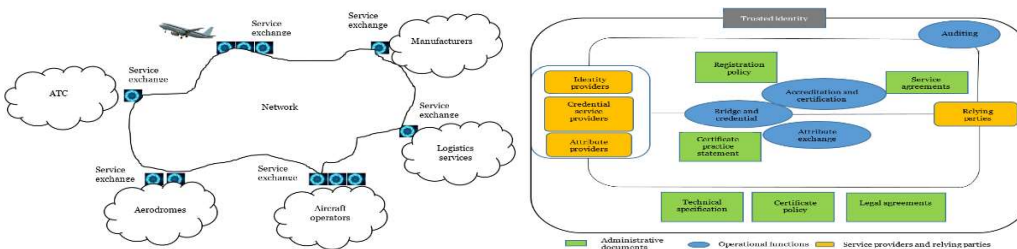
An international aviation trust framework is composed of two main elements: network management and identity management.

PhD student
Saulo José da Silva

PhD program
Aeronautical Engineering (UBI, University of Beira Interior)

Supervisor
Jorge Reis Silva (UBI, University of Beira Interior; CERIS, IST, University of Lisbon)

Co-supervisor
-

Period
2018-2022

Funding
-