PROJECT

vACCINE

AeronautiCal Cyber INtrusion dEtection mechanism

Funding: European (Horizon 2020)

Duration: Oct 2019 - Sep 2021

Status: Complete

Total project cost: €713,885

EU contribution: €499,720

Call for proposal: H2020-CS2-CFP09-2018-02

CORDIS RCN : 225392

Objectives:

ATC use of datalink is widely expanding over the years. Data communications are a key enabler sustaining SESAR/NextGen services, deployment being planned in the 2020+. Legacy data transmission is not encrypted for existing datalink capabilities and protocol. As a consequence, it is very hard to identify if failure is a malfunction or an attack.

However, civil aviation is an increasingly attractive target for cyber-attacks. New technologies such as e-enabled aircraft and modern CNS/ATM systems, together with trends towards greater connectivity, reliance on technology, common infrastructure underpinned with common technologies with common standards, etc. ... are changing the risk landscape of the aviation system.

The consequences of a potential cyber-attack in civil aviation are wide and can include:

1. (i) Lost of trust in new systems & concepts, limiting their successful deployment;
2. A 'domino effect' of failures across connected systems or common components;
3. Closure of the air traffic management system for unpredictable periods; ...

Since there is not a 'silver bullet' technology that will secure the aeronautical domain, it is essential to:

1. Investigate measures to make the current systems more resilient against cyber-threats
2. To establish effective and automated solutions for intrusion detection;
3. Promote its implementation worldwide and build trust across stakeholders.

Considering aforementioned challenges, the vACCINE Project aims to design an aircraft onboard security filter with an accuracy level of intrusion detection compatible with cyber protection objectives. The objective is to check/control data from the ground domain before authorizing them to enter the avionics domain not to compromise this level of safety.

Based modern digital transformation concepts and cyber-security technologies, the Project will deploy an innovative approach to catalyse the resilient of existing aeronautical communication systems against cyber-threat.

Parent Programmes:

H2020-EU.3.4. - Horizon 2020: Smart, Green and Integrated Transport

Institute type: Public institution

Institute name: European Commission

Funding type: Public (EU)

Other programmes: JTI-CS2-2018-CfP09-SYS-01-11 - Machine learning to detect Cyber intrusion and anomalies

Lead Organisation:

Gmvis Skysoft Sa

Address:
Av. D.joao Ii Lote 1.17.02, Torre Fernao Magalhaes 7°
1998025 Lisboa
Portugal

Organisation Website:
http://www.skysoft.pt

EU Contribution: €300,672

Partner Organisations:

X/open Company Limited

Address:
FORBURY ROAD APEX PLAZA
READING
RG1 1AX
United Kingdom

Organisation Website:
http://www.opengroup.org

EU Contribution: €199,048

Technologies:

"Electromagnetic attack detection devices and processes"""

Development phase: Research/Invention

STRIA Roadmaps: Other specified

Transport mode: Air transport

Transport sectors: Freight transport

Transport policies: Safety/Security, Digitalisation

Geo-spatial type: Other