CYBERSECURITY

© Athens International Airport

Security of Air Transport Infrastructure of Europe

SATIE

- SATIE has been developed to combat the persistent issue of airports cyber security
- Holistic approach to threat prevention, detection, response and mitigation in airports, while guaranteeing the protection of critical systems, sensitive data and passengers
- SATIE aims to integrate, harmonise and enhance security management at airports for all stakeholders

AIRBUS

Concept and objectives

Disruptions in airport operations may result from physical and/or cyber-attacks as well as their interconnected systems. Recent events demonstrate an increase of combined physical and cyber threats. A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent airport systems.

SATIE:

- Aims to integrate, harmonise and enhance security management at airports for all stakeholders
- Conducts cyber-physical risk assessments related to critical systems-of-systems
- Integrates solutions from the physical and cyber security spheres

SATIE has been developed to combat the persistent issue of airports cyber security through:

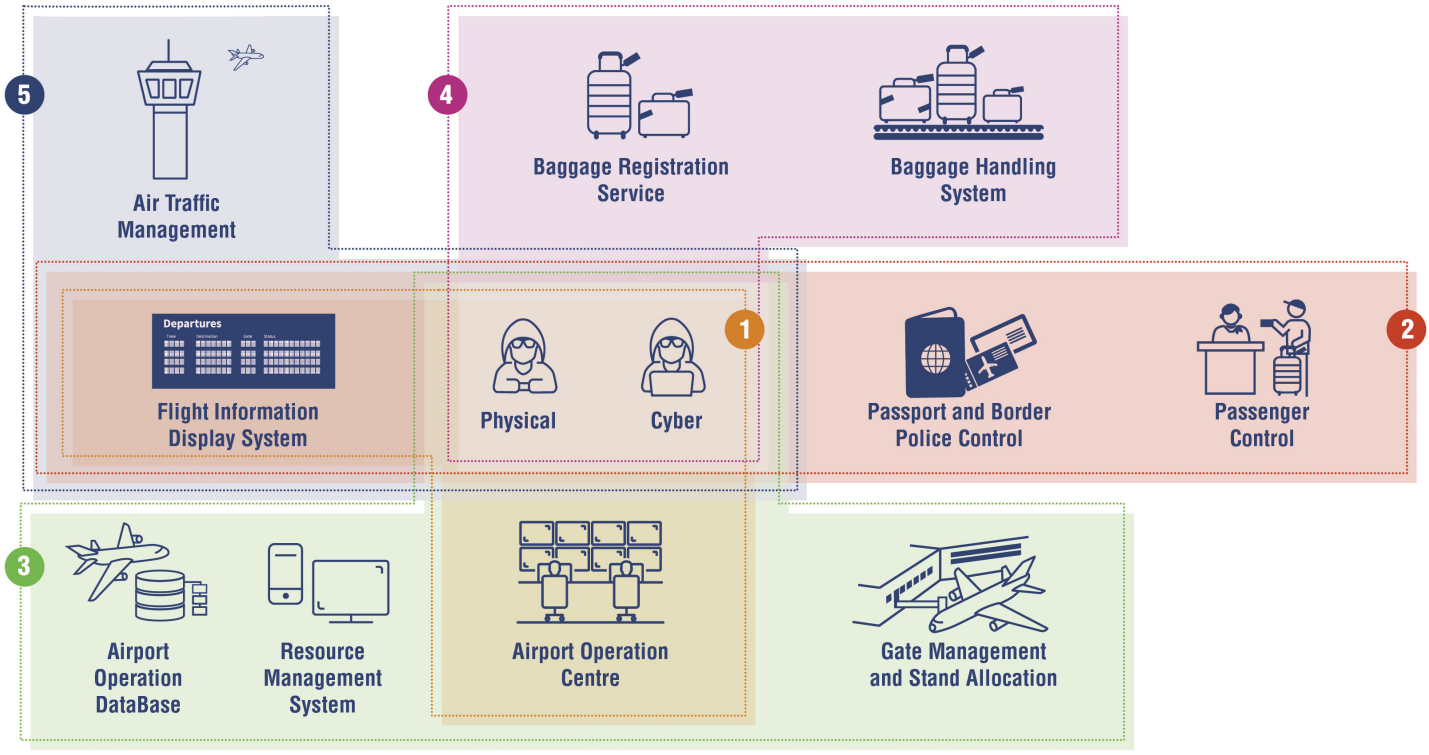
A holistic approach to threat prevention, detection, response and mitigation in airports, while guaranteeing the protection of critical systems, sensitive data and passengers

A combination of an interoperable toolkit that improves cyber-physical correlations, forensic investigations and dynamic impact assessment - and has the capability to counteract the new and increasingly complex cyber-physical threats that airports are currently facing

A way to a new generation of Security Operations Centres (SOC) that can be included in a comprehensive airport security policy

A project's applicability to real-life scenarios being validated through demonstrations in 3 European Airports (Zagreb, Croatia; Milan, Italy; and Athens, Greece)

5 Representative scenarios of cyber-physical attacks



1 Cyber-physical attack targeting passengers' security

2 Disturbance of the passenger controls

3 Compromising of the Airport Operations DataBase

4 Disorganisation of Baggage Handling Services

5 Endangered Air Traffic Management

Our contribution

In addition to our role as the **design authority** of the SATIE project, we act as **capability leader** for the correlation engine that will be at the very heart of the **cyber-physical SOC capacity.** It will prevent complex blended threats from getting through the various layers of defence. We are also responsible for **managing incidents** and can offer our **CyberRange** services.

Why does SATIE project matter

Airport and Aircraft Companies are targeted by cyber-attacks:

- In March 2018 a ransomware in **Atlanta Airport** encrypted multiple official computers and forced the airport to shut off its internal Wi-Fi network as a security measure to avoid ransomware spreading
- In April 2019, **Cleveland Airport** has been affected by publicly unreported ransomware preventing the display of baggage and flight information screens
- A cyber-attack occurred on the IT network of **RavnAir in Atlanta,** in December 2019, targeting the maintenance system of a specific aircraft type. The company had to shut down and knock out every part of the IT network as well as computers and servers. RavnAir had to cancel 8 flights, a few others were delayed and the company was affected for at least one month
- In March 2020, a hacking group infiltrated into the network of **San Francisco's International Airport** and maliciously injected code into the websites to steal the user credentials used by employees

18 participants from 10 European countries

Austria

Frequentis AG

Croatia

Zagreb Airport

France

Airbus CyberSecurity
Alstef Automation
Idemia Identity & Security France

Germany

Deutsches Zentrum für Luft- und Raumfahrt e.V, Institut für Flugführung
Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut

Greece

Athens International Airport S.A
Kentro Meleton Asfaleias
Satways

Italy

Network Integration and Solutions SRL
Società per Azioni Esercizi Aeroportuali

Poland

ITTI sp. z.o.o.

Portugal

Inov Inesc Inovação
Instituto Superior de Engenharia do Porto (ISEP-GECAD)

Slovakia

Ustav Informatiky, Slovenksa Akademia Vied

Spain

Eticas Research and Innovation
Teclib Spain SL

HORIZON 2020: ec.europa.eu/programmes/horizon2020
SATIE: satie-h2020.eu
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Programme co-funded by the
EUROPEAN UNION

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com