Project Goal

Disruptions in operation of airports may result from physical and/or cyber-attacks and their interconnected systems. Recent events demonstrate an increase of combined physical and cyber-attacks. A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent airport systems. Budgetary constraints on both public and private sectors mean that new security solutions must be more accurate, efficient and cost-effective, and possibly more automated than the ones currently available.

Concept and approach

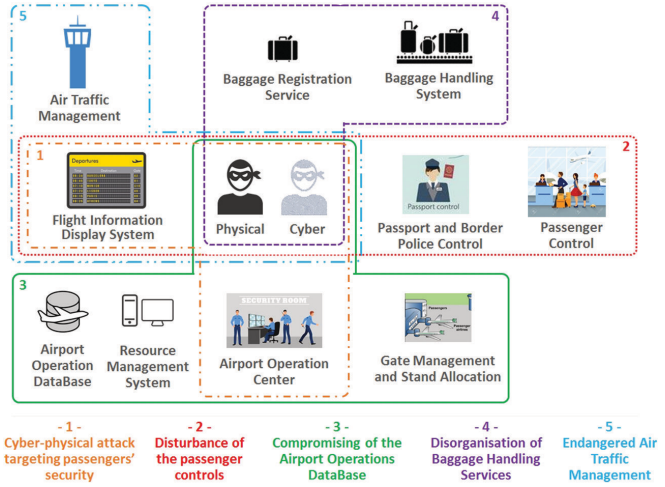
The SATIE overall concept aims at integrating, harmonizing and enhancing security management at airports for all stakeholders. SATIE examines cyber-physical risk assessment related to critical systems-of-systems. SATIE also integrates solutions from the physical and cyber security spheres.

Main project events

Three demonstrations will be conducted at three different international airports (Croatia, Greece and Itlay).

SATIE Scenarios

Five representative scenarios for the validation of the SATIE platform are developer, prepared and executed.



Objectives

- Identify main areas of security improvements in airports.
- Improve risk assessment methods for complex attack scenarios.
- Improve cyber and physical threat correlation, prevention, detection, response and mitigation on airport assets.
- Carry out operational demonstrations in real conditions.
- Foster dynamic airport security standards

Partners

Deutsches Zentrum für Luft- und Raumfahrt (DLR)
AIRBUS
teclib'
iTTi
inov inesc • inovação
Ústav Informatiky Slovenská akadémia vied
IDEMIA
FREQUENTIS FOR A SAFER WORLD
satways
eticas foundation
ATHENS INTERNATIONAL AIRPORT ELEFTHERIOS VENIZELOS
MZLZ Međunarodna zračna luka Zagreb Zagreb International Airport
ALSTEF
NIS network integration & solutions
Fraunhofer EMI
isep Instituto Superior de Engenharia do Porto
SEA Milan Airports
KEMEA