EASA
European Union Aviation Safety Agency

CYBER - Aviation resilience – cybersecurity threat landscape

Contractor

Deep Blue SRL

Consortium Members

Airbus Protect GmbH

Contract period

29/07/2024 - 29/09/2026

Budget

1.300.000€

Scan the QR code or click here
to visit the webpage of this project

Background & main objectives:

The research project CYBER has received funding through the Horizon Europe Work Programme 2023-2024.

The aviation industry is increasingly reliant on sophisticated information technology (IT) systems to support its operations. This growing reliance on IT has also made the industry a more attractive target for cyberattacks. In recent years, there have been a number of high-profile cyberattacks on aviation systems, including attacks on airlines, airports, and air traffic control systems. These attacks have raised concerns about the potential for cyberattacks to disrupt aviation operations and cause significant safety risks.

CYBER aims to identify cybersecurity threats having potential negative impact on the safety of flight operations. CYBER will investigate all **connected systems, both on the aircraft and on the ground**, that rely on external digital signals or services like satellite communications, or Position Navigation and Time (PNT). It will also look at systems used for controlling, navigating, managing, and maintaining the aircraft, as well as other types of operations such as getting the flight ready.

Instead of focusing on specific designs, **CYBER will examine general architecture and concepts for aircraft, ground, and space-based systems.** Evaluations will be done through simulations that involve, as much as possible, the whole infrastructure. The main goal of this research is to increase our understanding of the risks to information security in aviation that could impact safety, and to identify potential and emerging risks.

Impacts & benefits

The identification of cybersecurity threats having potential negative impact on the safety of flight operations will contribute to the on-going implementation of a roadmap towards a more resilient aviation system by ensuring that cyber risks are considered during aircrafts design, development and operation and then controlled in order to avoid adverse effects on citizens' safety.

This project is funded from the European Union's Horizon Europe research and innovation programme.

EASA
European Union Aviation Safety Agency

CYBER - Aviation resilience – cybersecurity threat landscape

Outcome

A better understanding of the information security risk in aviation having potential negative impact on safety. This knowledge should contribute to the on-going implementation of a roadmap towards a more resilient aviation system:

- → **Short-term:** Identification of critical areas where contingency measures should be defined, prioritised and disseminated to the impacted stakeholders;
- → **Mid-term**: Identification of areas where design changes that could improve the resilience of the aviation system should be defined, prioritised and disseminated to the impacted stakeholders;
- → **Long-term**: Identification of areas where further knowledge is needed, either via specific studies or research projects.

Output

- → A **risk assessment methodology** that enables a comprehensive and consistent means to evaluate information security risk having a potential impact on aviation safety;
- → A current and future **information security risk landscape** having potential impact on aviation safety;
- → **Summary of threats and their potential harmful impacts to safety** that should be considered by authorities and organisations by order of priority;
- → **Preventive and mitigative barriers** development, either by security or safety measures, including awareness campaigns, dedicated training, behavioural human aspects, specific policies, that would contribute to the resilience against identified cybersecurity threats;
- → **Assessment of emerging technologies and trends** to ensure aviation readiness for future potential threats, and proposal for specific studies or research projects.

Work packages (WP)

WP1 - Cybersecurity Risk Assessment: The objective of this task is to determine the most effective method for identifying and mitigating potential information security threats that may materialise into hazards for aviation safety.

WP2 - Survey of existing publications on cybersecurity risk: The objective of this task is to gather a comprehensive understanding of the current information security risk landscape in order to develop robust informational foundations upon which the research strategy can be refined.

WP3 - Impact assessment on safety of cybersecurity threats: The objective of this task is to understand the potential impact of each information security threat, in particular its potential to cause, or contribute to a serious incident or accident in aviation.

WP4 - Risk and residual risk: The objective of this task is to provide a technical evaluation of the threats, ranked by their adverse impact on safety as well as to provide a list of preventive and mitigative barriers to treat the risks identified during the assessment.

WP5 - Conclusions, recommendations, implementation roadmap and cost-benefit analysis: The objective of this task is to produce a final report consisting of a list of recommendations and a strategic roadmap for the implementation of the contingency measures identified.

This project is funded from the European Union's Horizon Europe research and innovation programme.