

AIRCRAFT CYBER SECURITY

Argus protects in-flight entertainment and connectivity systems against cyber attacks



According to the EU Aviation Safety Agency, "Aircraft systems and parts are increasingly connected, and those interconnections are susceptible to security threats. These threats have the potential to affect the airworthiness of an aircraft due to unauthorized access, use, disclosure, denial, disruption, modification or destruction of electronic information or electronic aircraft system interfaces "[1]. The most vulnerable systems to attack are the in-flight entertainment and connectivity (IFEC) systems, which are connected to the Internet.

Argus IFEC Protection protects vulnerable IFEC systems from cyber attacks:

EVERYTHING YOU NEED TO PROTECT

Argus IFEC includes six modules that operate stand-alone or in unison to provide optimal protection



CONTROL FLOW INTEGRITY
Prevent memory corruption attacks (e.g. buffer overflow) and program flow hijacking



SYSTEM LIMITER
Leverage OS hardening by blocking unauthorized processes



IFEC NETWORK PROTECTION
Detect and prevent malicious network traffic in real time



PLATFORM INTEGRITY
Prevent the introduction of malicious and unauthorized code



ADVANCED THREAT DETECTION
Uncover security policy deviations and grant autonomous response to an identified threat by leveraging advanced detection heuristics



SECURED LOGGER
Log security related events to enable cross-fleet monitoring, investigations, and forensics

THE ARGUS IFEC ADVANTAGE



MULTIPLE INDEPENDENT PROTECTION LAYERS



CUSTOMIZED TO YOUR NEEDS



TESTED AND IN PRODUCTION IN THE AUTOMOTIVE INDUSTRY



THREAT AGNOSTIC



ALWAYS-ON OPERABILITY



EASY TO DEPLOY

MORE ARGUS CYBER SOLUTIONS FOR IFEC PROVIDERS

Argus offers IFEC providers a SIEM solution, already in production in the automotive industry, and an array of consulting services to maximize the cyber resilience of IFEC systems:

ARGUS SIEM



MONITORS
SECURITY LOGS



ANALYZES
SUSPICIOUS ACTIVITIES



GENERATES INSIGHTS
FROM THE ENTIRE FLEET

ARGUS CONSULTING SERVICES



SECURITY
REQUIREMENTS



RISK
ASSESSMENTS



VULNERABILITY
RESEARCH



PENETRATION
TESTING

ARGUS - POSITIONED TO ADDRESS AIRCRAFT CYBER SECURITY

ARGUS IS A GLOBAL LEADER IN AUTOMOTIVE CYBERSECURITY -

Argus repeatedly outperforms competitors at customer evaluations

INDEPENDENT SUBSIDIARY OF CONTINENTAL -

Continental offers Argus solutions pre-integrated into all its connected automotive electronics components.



ARGUS ADDRESSES AVIATION'S UNIQUE CYBER SECURITY CHALLENGES -

Our best-of-class automotive cyber solutions, developed using an extensive knowledge base and resulting in numerous granted and pending patents, are being applied and further innovated upon specifically for the aviation industry.

AUTOMOTIVE CYBER SECURITY MEETS COMMERCIAL AIRCRAFT NEEDS -

The Argus research team has performed extensive research on technologies widely used in aviation, such as CAN bus (used in ARINC 825), ethernet (used in ARINC 664 or IFE), and operating systems like Linux, Android, and proprietary OS.

ABOUT ARGUS CYBER SECURITY

Argus, a global leader in automotive cyber security, provides OEMs, Tier 1s and fleet operators, scalable, end-to-end solutions and services that protect private and commercial vehicles against cyber attacks. In addition, Argus provides a software updates over-the-air (OTA) solution to enable OEMs to deploy software and security updates throughout the vehicle lifespan.

Ranked number one in third-party evaluations, Argus technologies are built on dozens of granted and pending automotive patents and rely on decades of experience in both cyber security and the automotive industry. Argus' customers include the world's largest OEMs and Tier 1 suppliers, and its partners include leading industry players. Founded in 2013, Argus is headquartered in Tel Aviv, Israel, with offices in Michigan, Silicon Valley, Stuttgart, and Tokyo and Shanghai.



For more information, go to www.argus-sec.com/aviation