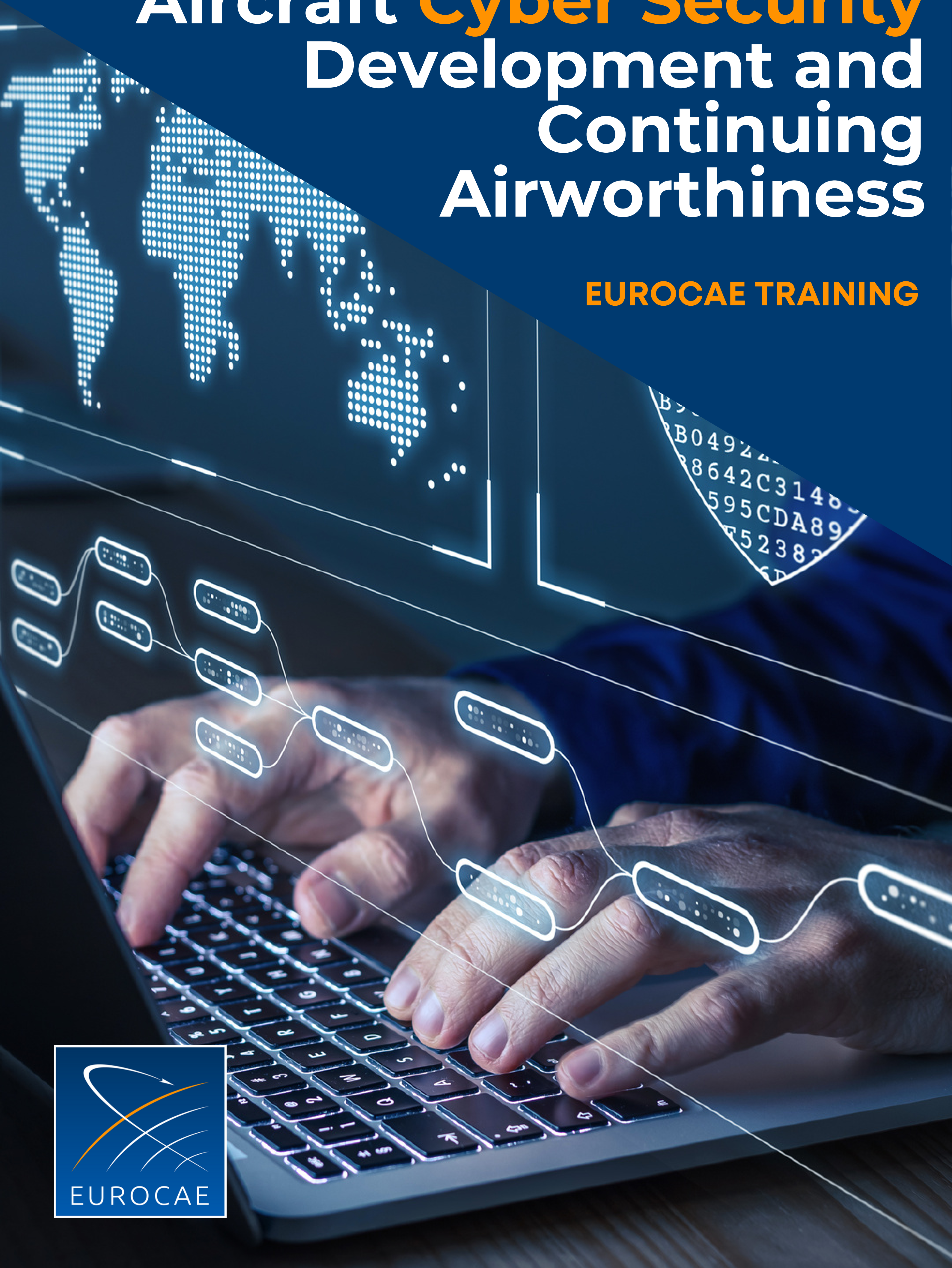
Aircraft Cyber Security Development and Continuing Airworthiness

EUROCAE TRAINING



EUROCAE

AVIATION CYBER SECURITY DEVELOPMENT

THE AIRCRAFT RISK PROFILE FOR CYBER-ATTACKS HAS CHANGED SIGNIFICANTLY WITH EVER INCREASING DIGITISATION AND CONNECTIVITY, SUCH AS E-ENABLED AIRCRAFT AND USE OF IP FOR INTERNAL AND EXTERNAL COMMUNICATION. TO ENSURE SAFETY AND SECURITY OF AIRCRAFT FROM CYBER-ATTACKS, EASA HAS PUBLISHED ED 2020/006/R TO INCLUDE CYBER SECURITY IN ALL CERTIFICATION SPECIFICATIONS (CS-23, CS-25, CS-27, CS-29, CS-APU, CS-E, CS-P, CS-ETSO).

In response to industry demand for a consistent practice in security by design for aircraft and to have harmonised approach in demonstrating compliance to the new aviation Cyber Security rules, EUROCAE WG-72 has developed three standards: ED-202A, ED-203A and ED-204A. The documents ED-202A and ED-203A provide a standard and guidance for developing aircraft, aircraft systems and parts from initial design to type certification. ED-204A provides the standard and guidance for maintaining airworthiness of aircraft from a Cyber Security perspective.

Who should attend?

This course is offered in two complementary parts. Participants can choose to attend either or both parts.

Aircraft Cyber Security Development

- Anyone working in a development or certification role exposed to Cyber Security within the design organisations and their suppliers – including design approval holders for Type Certificates in Airplanes, Rotorcraft, Engines, Propellers; design approval holders for Supplemental Type Certificates (STC); Design Approval Holders for (European) Technical Standard Orders (ETSO/TSO); and the suppliers of systems, software and hardware to any of the Design Approval Holders.

Aircraft Cyber Security Continuing Airworthiness

- Anyone working in design organisations in departments issuing Security Operator Guidance or Instructions for Continued Airworthiness and anyone in airlines, operators and maintenance, repair, overhaul (MRO) organisations in a cyber capacity – whether IT, operational or maintenance.
- Anyone working in aviation (airport, ANSP, airline, manufacturing industry (developing, producing or maintaining aircraft) plus regulatory and industrial audiences, who needs to deal with Cyber Security as part of their day-to-day activities.

The course content is structured for all background in these roles – whether IT with a security background, aviation backgrounds in system, software or hardware development or aircraft certification.

Course content

Aircraft Cyber Security Development ED-202A / ED-203A

- Cyber threats in aviation addressed in development
- The current Cyber Security regulatory landscape affecting aviation development
- Aircraft Security by Design
- Cyber Security Objectives for compliance demonstration
- Product Change
- Cyber Security Certification Plans
- Future developments

Aircraft Cyber Security Continuing Airworthiness ED-204A

- Cyber threats in aviation addressed in operation
- The current Cyber Security regulatory landscape affecting aviation operation
- Maintaining Cyber Security Continuing Airworthiness
- Aircraft Cyber Security Plans
- Future Developments

Learning objectives

The purpose of the training is to enable participants to adopt a standards-led approach to Cyber Security in aviation and to understand Cyber Security regulations for development and operation of aircraft, aircraft systems and constituent hardware and software. The participant will be able to:

Aircraft Cyber Security Development ED-202A / ED-203A

- Understand the new Cyber Security rules in all Certification Specifications and the associated AMC 20-42
- Establish a Cyber Security certification plan appropriate for the scope of the development activity
- Establish a Cyber Security development and verification plan with all activities and artefacts for Cyber Security certification
- Perform risk analysis for aircraft and aircraft systems
- Understand the Security Assurance Levels of ED203A and difference in allocation and application to DAL of ED12C, ED79A and ED80
- Understand some best practices in aviation development
- Understand the SAL objectives and demonstrate means of compliance to the objectives

Aircraft Cyber Security Continuing Airworthiness ED-204A

- Understand Cyber Security rules for operation of aircraft and for airlines
- Establish an Aircraft Cyber Security Plan
- Establish and demonstrate means to secure aircraft and associated ground operations
- Understand and manage Instructions for Continuing Airworthiness
- Understand how an Aircraft Cyber Security Plan can integrate with an Airline Information Security Management System

Benefits of attending

- Participants will gain access to the tools and understanding to use available standards to manage cyber risk in an aviation context in a standards-led way (which in itself brings many additional benefits)
- Learn best practice on auditing and certification
- Instructors are leading experts on aviation Cyber Security and regulations
- Share experiences with colleagues from other aviation stakeholders/countries
- Extensive course handouts including ED-202A, ED-203A and ED-204A
- Ideal distance learning programme to allow training at home or in the office
- Certificate of completion of the course

Course format: online

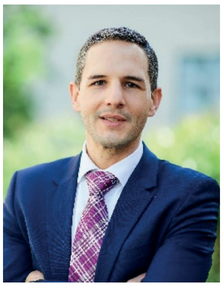
The training will be led by experienced Cyber Security experts **Hannes Alparslan** and **Stefan Schwindt**. The interactive sessions are subdivided into five half day sessions and incorporate several group exercises that shall facilitate learning and networking.

Digital workbooks are provided with all course materials and further reference material useful in daily work as well as complimentary copies of the ED standards. Note: the digital workbooks contain materials for students to prepare for each lesson

Terms and conditions

For terms and conditions please visit the EUROCAE website under https://www.eurocae.net/training/terms-and-conditions/

Trainers:



Hannes Alparslan works as Project Officer Aviation Cyber at European Defence Agency. His responsibilities within EDA include the establishment of a comprehensive approach to Cyber security in military aviation to improve resilience of ground and airborne platforms and to ensure that military requirements are duly considered on EU and international level, including in the increasingly important areas of standardisation and regulation.

He has been dealing with Information and Communication Technology for almost 20 years.

Before joining EDA, Hannes enjoyed 7 years at the Austrian Air Navigation Service Provider (ANSP), Austro Control with responsibilities including analysis of requirements towards and advising the management on strategic developments for the ATM/ATC system to improve overall effectiveness, efficiency and to ensure the future-readiness of the organisation.

He holds a degree in Electrical Engineering and a Master's degree in Information Systems Management with a focus in Cyber security and Forensics.

Since 2020, Hannes acts as trainer / lecturer for the EUROCAE courses related to Aviation Cyber security

Dr. Stefan Schwindt is the Director of Icarus Cyber security Consulting and Training. He has been in active in aerospace in academic and industry positions for over 16 years working covering many technical fields. His work has covered safety and reliability of systems and equipment, environmental testing, certification and product security in civil and military aviation.

He is active in the European and US industry organisation activities on civil aviation cyber security, co-authoring various recommendation reports. He has been representing the manufacturing industry at the European Strategic Coordination Platform for aviation cyber security rulemaking and the European Cyber security for aviation Standards Coordination Group.

He holds a Master in Aerospace Engineering, a doctorate in Engineering Science and an executive MBA.

Since 2020, Stefan acts as a trainer / lecturer for the EUROCAE courses related to Aviation Cyber security.