EUROCAE ONLINE TRAINING CATALOGUE

Q1-Q2 / 2021

Aircraft Cyber Security Development and continuing airworthiness

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

Trainers

Hannes Alparslan works as Project Officer Aviation Cyber at European Defence Agency. He has been dealing with Information and Communication Technology for almost 20 years.

Dr. Stefan Schwindt is the Director of Icarus Cybersecurity 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.

Course Fees

Aircraft Cyber Security Development and Continuing Airworthiness (combined format):
EUR 1.440 excl. VAT / EUROCAE members
EUR 1.800 excl. VAT / non-EUROCAE members

Aircraft Cyber Security Development only:
EUR 1.280 excl. VAT / EUROCAE members
EUR 1.600 excl. VAT / non-EUROCAE members

Aircraft Cyber Security Continuing Airworthiness
EUR 320 excl. VAT / EUROCAE members
EUR 400 excl. VAT / non-EUROCAE members

Next dates

22 March - 25 March 2021
21 June - 25 June 2021

For any additional information please contact Elena Marzac, Communication and Training Officer at elena.marzac@eurocae.net. For registration please follow the LINK.

Cyber Security management for aviation organisations

CIVIL AVIATION IS AN INCREASINGLY ATTRACTIVE TARGET FOR CYBER-ATTACKS. NEW TECHNOLOGIES SUCH AS E-ENABLED AIRCRAFT, NEW GENERATION CNS/ATM SYSTEMS AND DRONES ARE CHANGING THE RISK LANDSCAPE OF THE AVIATION SYSTEM.

At the same time, there is growing demand for guidance and leadership in cybersecurity, where EUROCAE WG-72 has brought a significant technical contribution through four EDs: ED-201, ED-202A, ED-203A and ED-204. Standards and guidance are proliferating in this space, which makes it potentially confusing for aviation stakeholders to know which is appropriate for what purpose. Guiding people through this maze is a key goal of this NEW two-day training course.

Who should attend?

Anyone working in aviation (airport, ANSP, airline, manufacturing industry) plus regulatory and industrial audiences, who needs to deal with cyber security as part of their day-to-day activities. This includes managerial, technical and operational people. Note that this training is not aimed at beginners nor at existing cyber security specialists who already have an in-depth understanding of the standards landscape.

Course content

- Cyber threats in aviation
- The current cyber security standards landscape
- ED-201 concepts and methods
- Cyber security auditing and certification
- Airworthiness standards
- Standards for securing operational technology
- Future developments

Learning objectives

The purpose of the training is to enable participants to adopt a standards-led approach to cyber security in aviation. The participant will be able to:

- Identify the principles and consequences of cyber security in the aviation environment.
- Describe how cyber security impacts different actors in aviation.
- Explain the scope and contents of ED-20X.
- Identify the interdependencies between the different standards by mapping the links between them, including ED-201 to ED-205, EN-16495, ISO27000 series, NIST standards, DOs and SAE documents.
- Select an appropriate standard, or set of standards, to adopt for specific aviation purposes.
- Research the process to follow and the information required for internal/external audits within an aviation context.
- Describe the top-level cybersecurity processes and aspects of certification in an ATM and aircraft context.

Benefits of attending

- Certificate on completion of the course.
- 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).
- ED-201 brought to life with classroom scenarios and exercises.
- Learn best practice on auditing and certification.
- Instructor is a leading authority on aviation cyber security and a certified lead auditor for ISO27001.
- Share experiences with colleagues from other aviation stakeholders/countries.
- Extensive course handouts including ED-201, ED-202, ED-203A, ED-204 and ED-205.
- Classroom format: Ideal learning environment at EUROCAE HQ in Saint-Denis (Paris area, France).
- Online format: ideal distance learning programme to allow training at home or in the office.

Course format: online

The training will be led by experienced cyber security experts Hannes Alparslan and Stefan Schwindt. It takes place of five half day sessions and will be interactive, including small group exercises to 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.

Trainers

Hannes Alparslan works as Project Officer Aviation Cyber at European Defence Agency. He has been dealing with Information and Communication Technology for almost 20 years.

Dr. Stefan Schwindt is the Director of Icarus Cybersecurity 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.

Course Fees

EUR 960 excl. VAT / EUROCAE members

EUR 1.200 excl. VAT / non-EUROCAE members

Next dates

17 - 21 May 2021

For any additional information please contact Elena Marzac, Communication and Training Officer at elena.marzac@eurocae.net. For registration please follow the LINK.