EUROCAE

CYBERSECURITY MANAGEMENT

FOR AVIATION ORGANISATIONS

Online training 5 HALF-DAYS

ED-201
ED-202A
ED-203A
ED-204A
ED-205

ED-201 - Aeronautical Information System Security (AISS) Framework Guidance

ED-202A - Airworthiness Security Process Specification

ED-203A - Airworthiness Security Methods and Considerations

ED-204A- Information Security Guidance for Continuing Airworthiness

ED-205 - Process Standard for Security Certification and Declaration of ATM ANS Ground Systems

AVIATION CYBERSECURITY TRAINING

NEW TECHNOLOGIES SUCH AS E-ENABLED AIRCRAFT, NEW GENERATION CNS/ATM SYSTEMS AND DRONES ARE CHANGING THE RISK LANDSCAPE OF THE AVIATION SYSTEM MAKING IT INCREASINGLY VULNERABLE FOR CYBER-ATTACKS.

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 five EDs: ED-201, ED-202A, ED-203A, ED-204A and ED-205. 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 five-half-days training course.

Who should attend?

Anyone working in aviation (airport, ANSP, airline, manufacturing industry developing, producing or maintaining aircraft) plus regulatory and industrial audiences, who needs to deal with cybersecurity as part of their day-to-day activities. This includes managerial people who need to understand the regulatory and standards landscape to establish secure organisations and processes. Note that this training provides an overview of standards and regulations and how they interrelate. This course is complemented by additional courses that will provide a more in-depth understanding of specific topics covered by individual standards.

Course content

- Cyber threats in aviation
- The current cybersecurity regulatory landscape affecting aviation
- The current cybersecurity standards landscape ED-20X standards for airworthiness and securing the aviation sector
- Cybersecurity auditing and certification
- Standards for securing organisations including information and operational technology
- Future developments

Learning objectives

The purpose of the training is to enable participants to adopt a standards-led approach to cybersecurity 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
- Understand which regulations apply to a particular aviation organisation
- 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

- 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 cybersecurity and regulations
- Share experiences with colleagues from other aviation stakeholders/countries
- Extensive course handouts including ED-201, ED-202A, ED-203A, ED-204A and ED-205
- 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 cybersecurity 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.

Day 1 and Day 2

1 - Introduction to aviation cyber security

- What is aviation cybersecurity?
- Key threats, risks and vulnerabilities
- What makes aviation different
- Who are the key stakeholders

2 - The Regulatory & Standards Landscape

- Overview of regulatory framework
- Industry standards (EUROCAE, RTCA, CEN, ISO, NIST etc.)

3 - Internal security

- What overall framework to use?
- Control catalogues
- What are the differences OT vs IT?

Day 3 and Day 4

4 - Assessment and certification

- Why do we need assessment and/or
- certification?
- ED-202A / ED-203A
- ED-205
- ISO 27001
- How to create assurance and trust
- How to approach an audit

5 - External security: supply chains and partnerships

- EN 16495
- ED-201

6 - Airworthiness security

- ED-202A
- ED-203A
- ED-204

Day 5

7 - Summary and assessment

How to book

Places are limited to a maximum of 20 people, so you are advised to book early online here:

https://www.eurocae.net/training/aviation-cyber-security-training/

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

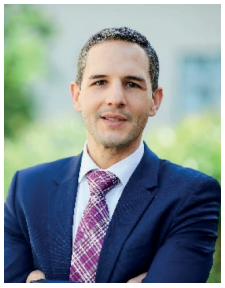
Course Fees

Online format: Cost: EUR1.200 (excl. VAT) for non-members / EUR 960 (excl. VAT) for Members

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 Cybersecurity 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 Cybersecurity and Forensics.

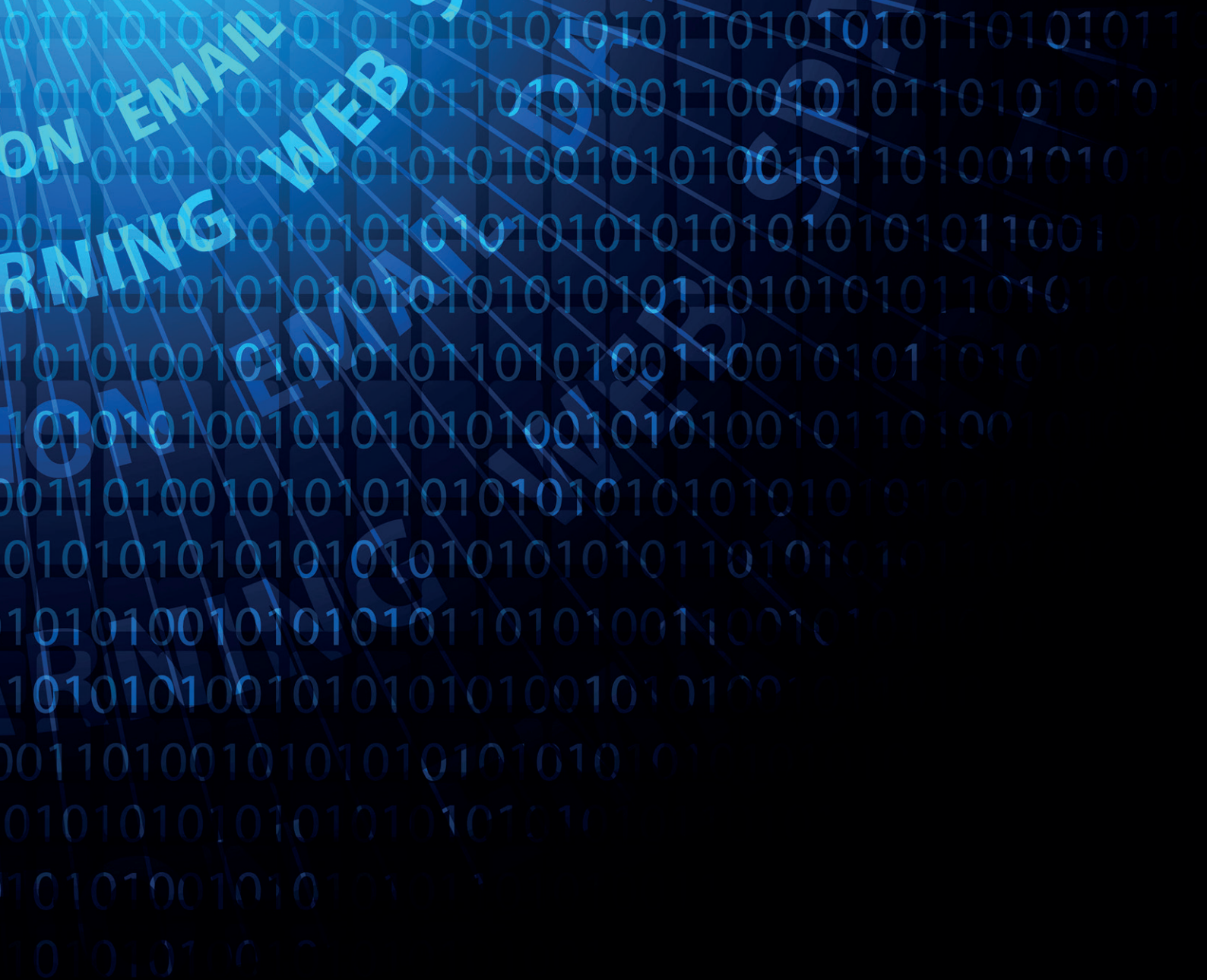
Since 2020, Hannes acts as trainer / lecturer for the EUROCAE courses related to Aviation Cybersecurity

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.

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



EUROCAE
9-23 rue Paul Lafargue
"Le Triangle" building
93200 Saint-Denis
T +33 1 49 46 19 65
www.eurocae.net