



DESIGN FOR SECURITY

Course Descriptions

This course will provide attendees with a solid foundation in the design of secure systems and products. We will define what cyber security means in a product development context and how it contributes to safe and reliable operation. To this end, we will need to clarify how security engineering differs from traditional safety and reliability engineering and how it is embedded into the overall systems engineering context. Although the entire product life cycle will be covered, emphasis will be put on the design and development phases, as these are the most important ones from the cyber security perspective. We will look into how to define a product security context and how to derive basic security architecture principles from it. We will then proceed with developing security risk assessment techniques and apply them to the system under design, i.e. we will elaborate on how risk assessment outcomes will result in security requirements that will need to be implemented in the system. Finally, we will discuss how security properties of a system can be validated and verified, both during the development and after entry into service. The course will focus on dependable systems in order to emphasize the intimate relation between safety and security.

Learning Outcomes

- Gain a good understanding of dependable systems and the role of security in their design and development
- Gain an understanding about the security implications of a system design
- Assess the business and project risks associated with specific design decisions
- Estimate the cost of security incidents
- For all stages of the product life-cycle, be able to outline the key elements associated with “designing for security”
- Have an overview of the tools and techniques employed by cyber security specialists when adopting a risk-based approach to security
- Have an appreciation of the security issues associated with software, human/system interactions, novel technologies, complex system of systems and autonomy

Who Should Attend?

- Design engineers needing to improve or refresh their product security knowledge to enhance their integration within a Systems Engineering team
- Safety engineers who need work together with security engineers on a common system design and have not yet been exposed to the topic
- Project and program managers wishing to understand how poor security engineering can lead to prohibitive business and project risks
- Engineering managers wishing to improve their specialist knowledge order to gain the most from their security team
- Business leaders wishing to understand their legal and moral responsibilities to ensure that products and systems are designed, commissioned and operated safely and securely

Course Rates

Early Bird: 1350 CHF | Regular: 1500 CHF

Duration

2 days

Delivered By



Stephan Marwedel

Stephan works as a product security engineer at Airbus commercial aircraft. In his work, he brings together diverse engineering disciplines, such as hardware and software engineering, mechanical engineering, safety and reliability and cyber security aiming at creating safe and secure solutions.

Stephan has more than 30 years of experience at software and systems engineer in diverse areas, such as chip design, secure networking, health care, online banking and logistics. He spend ore than half of his professional life at Airbus commercial aircraft working as a systems engineer on aircraft communication systems and as an product security engineer on communication and recording systems as well as landing gear systems. He is actively involved in developing security standards by particiating in international working groups at EUROCAE, AEEC and SAE.