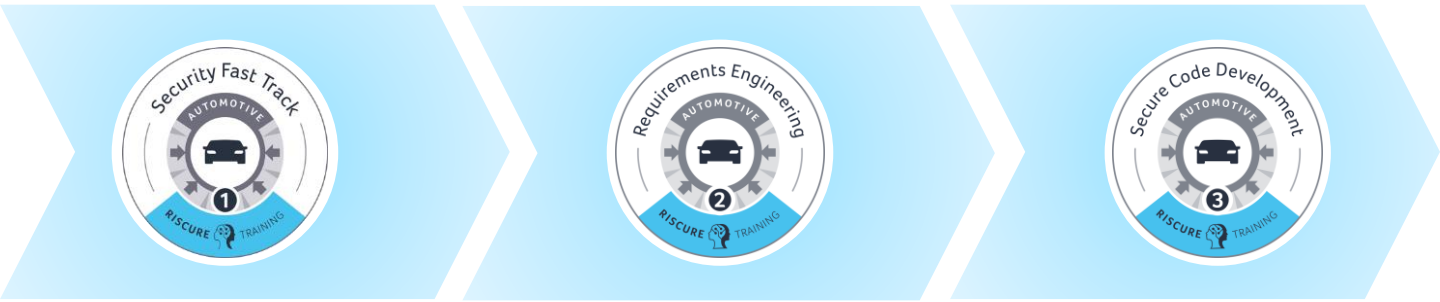
Effective Technical Decision Making for Automotive Security

An automotive E/E solution that does not protect from an adversarial action cannot be considered state-of-the-art. Breached security of a safety-critical component leads to potential liability and may result in a costly delay in production because you cannot meet your functional safety requirements any longer. Based on years of experience developing and certifying secure devices and software across various industries, Riscure has created a dedicated interactive Automotive Security Training.
The training bridges the gap between formalized safety frameworks such as ISO 26262, SAE J3061-20161 and the upcoming ISO/SAE 21434 and the best practices in security. It provides three levels of security insight, and covers the following areas of expertise:



Part 1:
Fast track your security
Adding security to a product is expensive. Learn about the typical lifespan of software and hardware solutions, the importance of testing and how you can reduce costs.

Part 2:
Security Requirements Engineering
Save time in learning how to adhere to the security requirements by getting an in-depth overview of the five most common TARA methodologies.

Part 3:
Secure code development
Explore techniques collected over 20 years of code reviews, to systematically discover vulnerabilities in code. Assess the impact of vulnerabilities for deploying a cost effective remediation plan.

Who Is This Course For?

If your job means you are responsible for at least two requirements from the following list, then you are a perfect candidate for this course:

- Interface with stakeholders to understand requirements, domains, and viable technologies.
- Advise the project team on key issues of functional safety in requirements engineering and management, especially during software design and architecture development activities.
- Create, maintain and refine all documents relating to security topics such as: security plans, security objectives and requirements, functional architecture, or requirements for hardware and software for automotive ECU development projects.
- Identify risks and quality issues, estimate effort, analyze requirements and establish priorities.
- Define architectural requirements and align them internally as well as with the customer.
- Integrate cybersecurity aspects into your existing safety engineering processes.

riscure

Decision Makers

300 EUR

Online course

1

Automotive: Security Fast Track

Adding security to a product is expensive. Some costs can be easily quantified (e.g., performance penalty in the product) while others (expertise and communication) are revealed in the process. Finding the optimum trade-off between the benefits of security features and their cost requires experience. You can speed up your learning process by reviewing the lessons learned from other industries such as payment and content protection. In a span of a few years, these industries have practically eliminated the threat of a professional hacking their products. In this course, we apply **lessons learned** from other industries to **fast track your automotive security.**

Benefits: You fast track your security by analyzing the lessons learned from other mature industries. In this 3 hour course, you learn how to use security terms and improve your understanding of security risks. You analyze requirements and establish priorities for building secure products and processes.

All the lessons we share in this short course are immediately actionable.

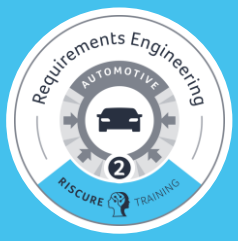
1 Learning Session Content

01 **INTRODUCTION.** We give an overview of automotive security events that shaped the industry. Next, we show how the industry is changing and compare it to other industries in order to highlight both similarities and unique challenges in automotive.

02 **TERMINOLOGY**. We establish a baseline of security terminology, to effectively discuss the rest of sessions, and to introduce relevant concepts.

03 **INDUSTRY SECURITY PRACTICES.** We look at the payment and content protection industry which have reached a mature security level. We analyze the evolution of the security practices in these markets.

04 **SAFETY VS SECURITY TESTING.** Security testing is fundamental to safety. We compare and contrast the steps involved in safety and security testing, and highlight the differences in processes and goals. We discuss how to integrate security in automotive development processes.



Decision Makers

300 EUR

Online course

2

Automotive: Security Requirements Engineering

Requirements are the ingredients for a good product but do not on their own lead to the expected results. The key is their interpretation and implementation. Modern product specifications in the automotive industry often include security requirements. Save time in learning how to adhere to the security requirements by getting an in-depth overview of the five most common TARA methodologies. In this module, we go over the details of each methodology and compare and contrast their strengths and limitations. We close off with a case study where we use a set of predefined security requirements. We follow a TARA process using the different available methodologies and propose technical specifications. We pay special attention to the meaning and effective implementation of these security requirements.

Benefits: You save money and time by accelerating the process of writing technical solutions that meet the OEMs' security requirements. You learn to ask the right questions and avoid common pitfalls in the implementation There is no way around the self-study of the methodologies, but we can give you a jumpstart and guide you through the entire process.

2 Learning Session Content

01 **SECURITY REQUIREMENTS.** We look at the role of security requirements, why they are issued and what it means to meet a security requirement. We give a semi formal definition of security requirements as outlined by SAE J3061.

02 **IMPLEMENTATION CHALLENGES.** While the goals of safety and security are analogous, the scope of security is broader than that of safety and the implementation process is different. Additional challenges include unfeasible, unrealistic requirements. Essential for correct implementation are assumptions, expectations and processes.

03 **TARA METHODOLOGIES.** After a brief description of the main five methodologies used for threat modeling: MITRE TARA, EVITA, STRIDE/DREAD, HEAVENS and Common Criteria (CC) we compare and construct their strengths and weaknesses.

04 **CASE STUDY.** We perform a mock-up TARA on a case study according to a subset of the previous mentioned methodologies.

Decision Makers

300 EUR

Online course

3

Automotive: Secure code development

Safety is critical for the automotive industry and software is a major component of a modern car. Coding guidelines such as MISRA-C promote best practices in developing safety-related embedded systems by providing rules and rationales for code development. Some MISRA-C rules have security implications, and it is important to understand why otherwise you will shoot yourself in the foot. In this training, we give examples of code that follows the MISRA-C rules but can be used to compromise the system. Starting from such an example, we illustrate the shortcomings of secure code development guidelines. We dive into the economics of secure coding and give you the resources to follow-up.

Benefits: We cannot promise that you learn to write secure code in 3 hours (we are still working on that!), but you will understand the shortcomings of secure coding guidelines. In addition, you will understand the cost of fixing vulnerabilities in the different stages of product development and get the tools to argue threat responses.

3 Learning Session Content

01

WHY MISRA-C COMPLIANT CODE MIGHT NOT BE SECURE CODE
Are architects aware that developers will bypass rules?
Example: dynamic memory allocation

02

SECURE CODING BEST PRACTICES (30MIN)
Lessons learned from 20 years of code reviews
Introduce and discuss secure coding guidelines
Legacy code
Protect your perimeter

03

WHY IT IS COST EFFECTIVE TO PRACTICE SECURE CODING DURING EARLY STAGES OF PRODUCT DEVELOPMENT
Vulnerability calculators
Throughput vs Quality dilemma? - work smart not fast

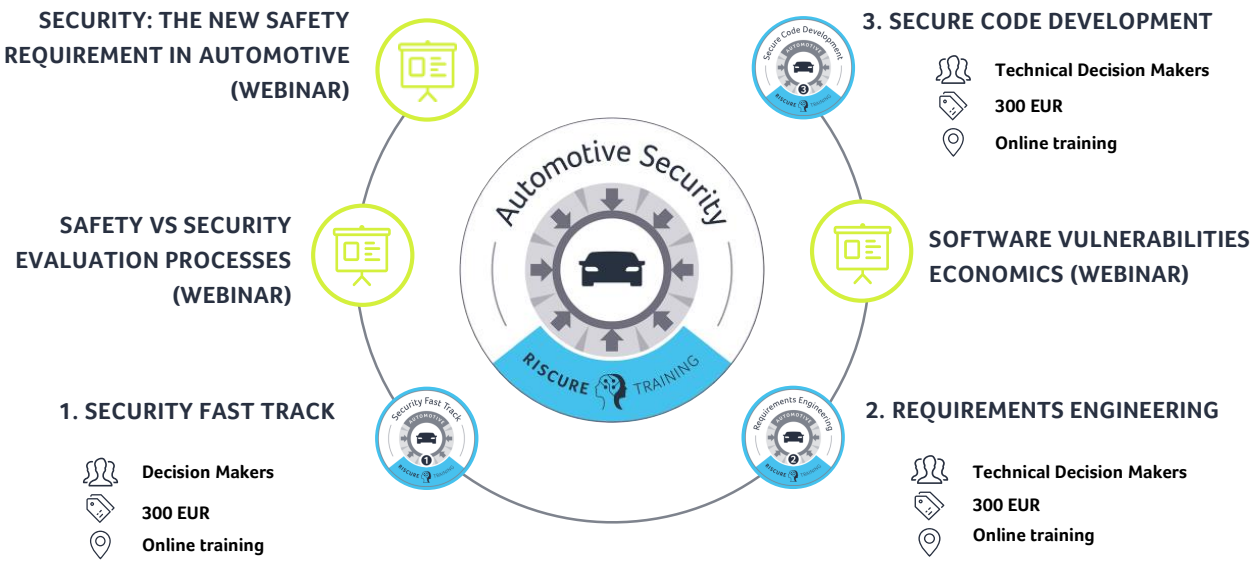
04

REAL WORLD CHALLENGES
Hunting vulnerabilities in large code bases
Linked vulnerabilities
Inherited vulnerabilities (e.g. libraries)

Course Structure

This course consists of three parts: an **instructor-led learning session**, time for completing **assignments and self-study**, and a **Q&A session**. The learning session is recorded and can be watched **anytime** after the official broadcast date. In the Q&A session we discuss any questions you might have related to the course or homework.

What Next?



Register here: https://www.riscure.com/training/automotive-security-online-training/

Features

01 ONLINE
Delft is beautiful, but traveling here takes time and money. We are offering this training online, so you can access it anywhere, anytime.

02 ACTIONABLE
All lessons in this short course are immediately applicable on the job.

03 COMPRESSED
We know you are busy so we don't beat around the bush and give you the information straight up.

04 AFFORDABLE
For only 300 EUR you get access to 3 hours of video content, downloadable training materials, and the possibility to ask questions to our experts.

05 INTERACTIVE
Watching an online course can test your patience. We break the content in pieces and add a healthy dose of interactive exercises.

riscure

WHAT ARE THE BENEFITS OF RISCURE TRAINING SERVICES?

We believe that learning by doing is the best way to develop your skillset. Our security training programs excel in being interactive with many hands-on exercises. Starting with creating a good conceptual understanding, we quickly move on to applying your knowledge to real-world examples and revisit concepts for optimal retention. The effectiveness of our approach is demonstrated by the consistently very high satisfaction scores we receive from our customers.

Knowledge programs designed to accelerate learning on embedded and connected system security:

Our courses are designed to help accelerate the time to market of your product. Our introductory programs provide critical insights for understanding security requirements, relevant attacker models, typical vulnerabilities and fundamental security mechanisms. Our specialized courses dive deep into one expertise area designed to deliver maximum insights in the minimum amount of time.

Up to date, practical content:

We make extensive use of our skills, knowledge and experience gained from working on hundreds of hardware and software security projects. We follow a rigorous process for content development in line with state-of the art methodology of instructional design. After each delivery, we document the lessons learned and update the content accordingly.

Some of the best trainers in the security industry:

Our trainers are experts in their field of training. All have a Msc or PhD degree in the area of embedded/connected systems and have gained extensive experience working as security analyst or developing security tools. All our trainers follow communication training and specialized training delivery courses to complement their expert field.

Flexible delivery, from classroom to online, including building learning into your company knowledge program or corporate university:

We offer self-directed and instructor led courses. Our self-directed courses are available anytime, anywhere. Our instructor-led courses can be provided both as virtual and class-room trainings internally at your location or in open sessions at one of our offices.

Our online programs are compatible with most training standards and can be replicated on your own servers or in your company's own program, allowing easy training of new employees or job changers as well as keeping security knowledge of your teams always up to date.