AUTOMOTIVE TARA TRAINING COURSE

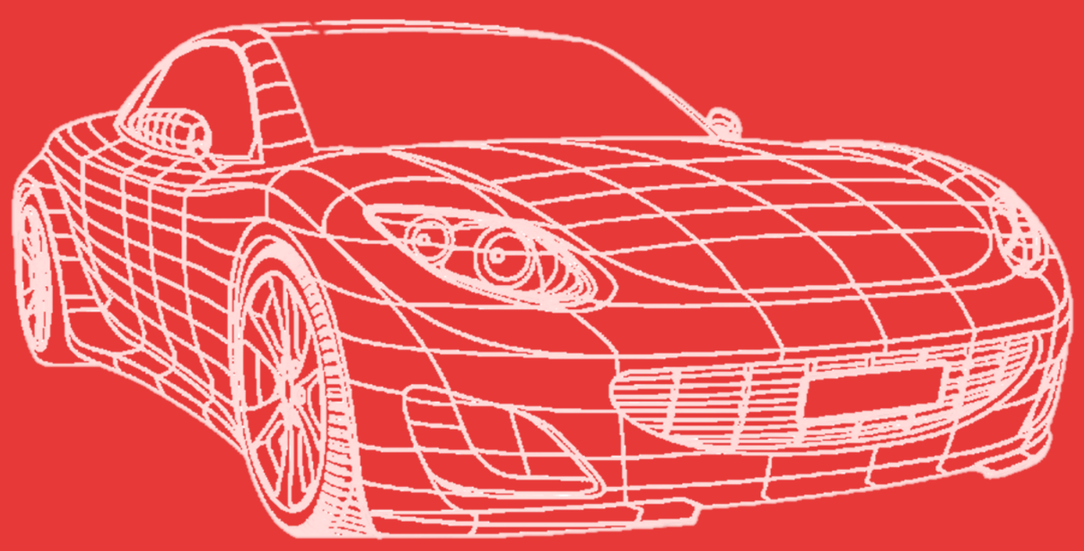
drivesec

WHAT CAN YOU EXPECT?

This course is designed for professionals in the automotive industry seeking to understand and implement **Threat Assessment and Risk Analysis** (TARA) methodologies. As vehicle technologies become increasingly connected and automated, the importance of identifying and mitigating potential risks to safety and security has never been greater, and, ultimately, this has become mandatory due to various regulations

In this course, participants learn the **fundamentals of TARA methodology**, including identifying threats, risk assessment techniques, and strategies for effective risk management in automotive systems. The course is based on standard ISO21434, Cybersecurity Vehicle Engineering, and through real-world case studies and practical exercises, it will explore the challenges faced by the industry in safeguarding vehicles and their components from cyber threats and other risks.

By the end of this course, you will have the skills and knowledge necessary to conduct thorough **risk assessments, make informed decisions regarding risk mitigation, and contribute to developing safer, more secure automotive technologies.**



AUTOMOTIVE TARA TRAINING COURSE

drivesec

The course will include the following **points:**

1

Cybersecurity Regulations and the Role of TARA

In recent years, the automotive industry has witnessed the establishment of stringent cybersecurity regulations aimed at protecting vehicles from potential cyber threats. These regulations, such as those outlined by the European Union Agency for Cybersecurity (ENISA) and the guidelines set forth by the International Organization for Standardization (ISO), emphasize the necessity for manufacturers to incorporate cybersecurity within the entire lifecycle of vehicle development. The role of Threat Assessment and Risk Analysis (TARA) is crucial in this context, as it provides a structured approach for identifying potential threats, assessing vulnerabilities, and determining the impacts of cyber incidents. By implementing TARA, automotive companies can comply with regulatory requirements while proactively enhancing the security posture of their vehicles.

The main international regulations will be analysed, in particular the UNECE Regulation 155, and the role of the TARA methodology within them and the results expected from such use are explored in depth.

2

General Aspects of Risk Assessment

Risk assessment is a critical process in various industries, including automotive, as it helps identify, evaluate, and prioritize risks to mitigate their impact effectively. The general aspects of risk assessment involve understanding the context in which the risks exist, identifying potential hazards, analysing the likelihood and consequences of these hazards, and determining appropriate risk mitigation strategies. In the automotive sector, this includes considering factors such as the connectivity of vehicles, software complexities, and user interactions. A comprehensive risk assessment facilitates informed decision-making, enabling manufacturers to allocate resources effectively while ensuring the safety and security of both vehicles and their occupants.

3

The TARA Methodology (ISO 21434)

The TARA methodology, as specified in ISO 21434, provides a systematic approach tailored for the automotive sector to address cybersecurity risks effectively. This methodology encompasses several key steps, including threat identification, vulnerability analysis, impact assessment, and risk prioritization, ultimately leading to the formulation of risk treatment strategies. By leveraging the TARA methodology, automotive stakeholders can ensure they systematically consider all relevant factors, including technological, operational, and human elements, when evaluating risks. The structured nature of ISO 21434 helps organizations establish consistent practices while complying with regulatory requirements and enhancing the overall resilience of their vehicle systems against cybersecurity threats.

The ISO 21434 standard, concerning the parts related to TARA, will be explained in detail, including the example proposed in the standard itself.

4

Application of TARA in a Practical Example

To illustrate the application of TARA, it will be considered a scenario involving a connected component of a vehicle. In this case, a TARA assessment starts by identifying potential threats, such as unauthorized access to vehicle data or manipulation of control systems. Following the identification, the analysis evaluate vulnerabilities in the software and hardware architecture that could be exploited by malicious actors. The impact of various attack vectors is assessed—considering outcomes such as loss of vehicle control or data breaches. Based on the analysis, prioritized mitigation strategies are considered to address the highest risks, such as implementing stronger encryption protocols or enhancing user authentication methods. This practical example demonstrates how TARA can guide automotive companies in making informed decisions that bolster their cybersecurity measures and safeguard their vehicles or components against potential threats.

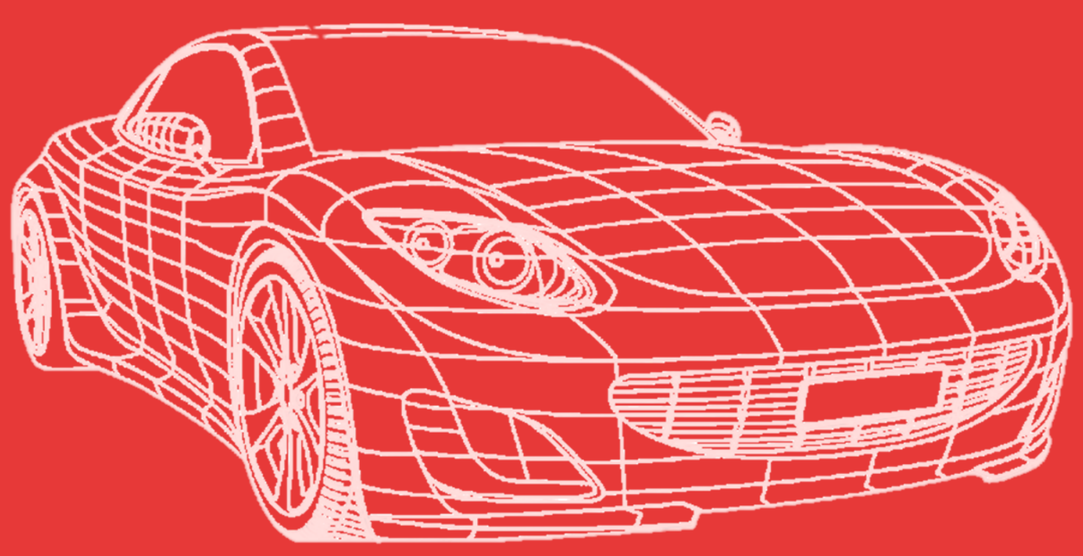
AUTOMOTIVE TARA TRAINING COURSE

THE PRACTICAL PART

After the description of the components, all the steps needed to complete the TARA analysis will be performed, using the tools provided by Drivesec:

- **Item definition**
- **Asset identification**
- **Threat scenario identification**
- **Impact rating**
- **Attack path analysis**
- **Attack feasibility rating**
- **Risk Value determination**
- **Risk treatment decision**

At the end of the course, participants can fill out a small questionnaire to self-assess their level of learning and will receive a proof of attendance.



Contact us at marketing@drivesec.com
And follow us on LinkedIn