TÜV Certified Automotive Cybersecurity ISO/SAE 21434 & Security Engineering Training: Level-2 (paid course)

Agenda VectorAcademy

Delivery Format:	This Course is offered in Classroom Format
Duration:	2 days (Basis Contents) + 1 day (AUTOSAR based advanced training, option)
Target Group:	For participants from automotive industry who want to learn and engage in cybersecurity-related work
Prerequisites:	V-Model for Automotive Software Development
Goal:	To understand the regulations and standards of automotive cybersecurity, be familiar with the concepts, methodologies and practices with regards to ISO/SAE 21434-based cybersecurity management systems, as well as knowledge of the basic principles and practice of security engineering and security testing. （option contents: In-depth understanding of the principles, applications, and configuration exercises of network security mechanisms in AUTOSAR）

1. Basic Contents (2 days)

Challenge Cybersecurity, Standards, Regulation and Terminology

- Introduction to industry trend and terminology
- Interpretation of standards and regulations (ISO/SAE 21434:2021, UNECE R.155, GB 44495-2024, etc.)

Cybersecurity Management and Governance

- Interpretation and best practice sharing of organizational cybersecurity management
- Interpretation and best practice sharing of project dependent cybersecurity management
- Interpretation and best practice sharing of distributed cybersecurity activities

Risk-based Cybersecurity and Cybersecurity Analysis

- Risk-based cybersecurity and its key focus
- Methodology, best practice sharing and exercises of TARA

Systematic Cybersecurity Engineering

- Introduction of Cryptography
- Security by Design – Guideline of Secure Coding
- Root of trust – Hardware Security Module (HSM)
- Introduction and experience sharing of Secure Update/Download/Flashing
- Introduction and experience sharing of Secure Boot
- Introduction and experience sharing of Secure Communication (SecOC)
- Introduction and experience sharing of Secure Diagnostics (0x27, 0x29)
- Introduction and experience sharing of Secure Logging

VECTOR

TÜV Certified Automotive Cybersecurity ISO/SAE 21434 & Security Engineering Training: Level-2 (paid course)

Agenda VectorAcademy

- Introduction to Adaptive AUTOSAR Secure Defense Mechanism (Secure Communication, Secure Diagnostics etc.)

Cybersecurity Verification and Validation

- Introduction to methodology , tools and sharing of best practices of Static Code Analysis
- Introduction to methodology , tools and sharing of best practices of Functional Testing
- Introduction to methodology , tools and sharing of best practices of Vulnerability Scanning
- Introduction to methodology , tools, sharing of best practices and practice of Fuzzing
- Introduction to methodology , tools, sharing of best practices and practice of Penetration

Cybersecurity for Post-development Phase

- Interpretation and best practice sharing of Production
- Interpretation and best practice sharing of End of Cybersecurity Support
- Interpretation and best practice sharing of Decommissioning
- Interpretation and best practice sharing of Continual Cybersecurity Activities
- Interpretation and best practice sharing of Cybersecurity Incident Response
- Interpretation and best practice sharing of Updates

Exam and Certification

- Vector Certificate: Take and pass the exam organized by Vector, Certificate of Level-2
- TÜV Certificate:
  - The prerequisite for taking the exam is completing Vector security training.
  - Take and pass the exam organized by TÜV for Level-1, Certificate of Level-1
  - Take and pass the exam organized by TÜV for Level-2, Certificate of Level-2
  - Certificate of Level-1 is the precondition for taking the Level-2 exam.
- No exam: Issue a Certificate of Completion from Vector

2. AUTOSAR based advanced (1 day, option)

Below contents are optional

Basic Concepts

- Basic concepts primitives
- Basic concepts keys
- Basic concepts jobs
- Basics AUTOSAR crypto stack

VECTOR

TÜV Certified Automotive Cybersecurity ISO/SAE 21434 & Security Engineering Training: Level-2 (paid course)

Agenda VectorAcademy

Walk-through Example: Cipher-based Message Authentication Code (CMAC)

- Show detailed configuration of crypto jobs for CMAC generation and verification
- Show configuration of the crypto stack (Csm, CryIf and Crypto driver)

Exercise (DaVinci Configurator)

- Configuration of the Crypto Stack (with SW Crypto Driver)
- Configuration of cryptographic keys
- Configuration of cryptographic jobs (encrypt and decrypt, MAC generation and verification)

Certificate

- Attendance time is not less than 80% of the course duration and exam passed