Cybersecurity for Connected and Autonomous Vehicles Training Course

Professional Development Training Course Outline

Category	Traffic Management & Road Safety	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Connected and Autonomous Vehicles represent a transformative shift in mobility, integrating advanced sensors, V2X communication, edge-computing systems, AI-based decision engines, and cloud-connected architectures. As vehicles become increasingly software-defined, their attack surface expands dramatically, exposing them to risks such as wireless intrusion, ECU manipulation, sensor spoofing, supply-chain attacks, and data-privacy breaches. Ensuring cybersecurity in this domain requires a multi-layered defense strategy aligned with global standards such as ISO/SAE 21434, UNECE WP.29 R155/R156, and best practices for secure OTA updates, threat modeling, and cryptographic communication.

The rapid evolution of intelligent mobility ecosystems spanning smart cities, 5G infrastructure, digital twins, and edge-cloud integration necessitates security frameworks that address both technical and regulatory dimensions. Cybersecurity for Connected and Autonomous Vehicles Training Course provides a comprehensive, hands-on understanding of securing CAV architectures. Participants will explore real-world attack scenarios, mitigation techniques, secure-by-design development, automotive penetration testing, security monitoring, and resilience engineering to prepare for the next generation of autonomous transportation.

Programme Curriculum

Cybersecurity for Connected and Autonomous Vehicles Training Course

Introduction

Connected and Autonomous Vehicles represent a transformative shift in mobility, integrating advanced sensors, V2X communication, edge-computing systems, AI-based decision engines, and cloud-connected architectures. As vehicles become increasingly software-defined, their attack surface expands dramatically, exposing them to

risks such as wireless intrusion, ECU manipulation, sensor spoofing, supply-chain attacks, and data-privacy breaches. Ensuring cybersecurity in this domain requires a multi-layered defense strategy aligned with global standards such as ISO/SAE 21434, UNECE WP.29 R155/R156, and best practices for secure OTA updates, threat modeling, and cryptographic communication.

The rapid evolution of intelligent mobility ecosystems spanning smart cities, 5G infrastructure, digital twins, and edge-cloud integration necessitates security frameworks that address both technical and regulatory dimensions. Cybersecurity for Connected and Autonomous Vehicles Training Course provides a comprehensive, hands-on understanding of securing CAV architectures. Participants will explore real-world attack scenarios, mitigation techniques, secure-by-design development, automotive penetration testing, security monitoring, and resilience engineering to prepare for the next generation of autonomous transportation.

Course Duration

5 days

Course Objectives

1. Understand the CAV cybersecurity landscape and emerging global threats.
2. Apply ISO/SAE 21434 and UNECE WP.29 regulatory requirements for secure vehicle design.
3. Analyze vehicle network architectures including CAN, Automotive Ethernet, and V2X protocols.
4. Identify vulnerabilities in ADAS and autonomous perception systems.
5. Perform threat modeling (HEAVENS, EVITA) for CAV components.
6. Implement secure communication protocols for V2V and V2I ecosystems.
7. Evaluate cryptographic key-management strategies for edge-connected vehicles.
8. Conduct automotive penetration testing and ECU security assessments.
9. Develop secure OTA update and firmware-integrity mechanisms.
10. Mitigate AI/ML cybersecurity risks in autonomous decision systems.
11. Implement zero-trust architecture for connected mobility environments.
12. Strengthen supply-chain cybersecurity for hardware and software components.
13. Design incident response and cyber-resilience frameworks for intelligent transportation systems.

Target Audience

1. Automotive cybersecurity engineers
2. ADAS and autonomous-vehicle developers
3. Vehicle network and embedded-systems engineers
4. Cybersecurity analysts and penetration testers
5. Automotive OEM and Tier-1 security managers
6. Smart-city mobility planners and ITS professionals
7. Compliance officers and regulatory specialists
8. IT/OT security teams supporting connected-mobility infrastructure

Course Modules

Module 1: Introduction to CAV Cybersecurity

- Evolution of connected and autonomous mobility
- CAV cybersecurity threat landscape
- Impact of digitalization and software-defined vehicles
- Overview of automotive cybersecurity standards

- Safety-security convergence principles
  Case Study: Bluetooth & remote-unlock radio attack on a connected vehicle platform.

Module 2: Vehicle Network Architecture & Attack Surfaces

- CAN, LIN, FlexRay, Automotive Ethernet overview
- ECU ecosystem and communication pathways
- Wireless attack vectors
- Sensor spoofing
- Cloud and edge computing vulnerabilities
  Case Study: Spoofed GNSS signals causing route manipulation in test fleets.

Module 3: V2X Security Fundamentals

- V2V, V2I, V2P communication protocols
- PKI and cryptographic requirements for V2X
- Authentication, authorization, and trust models
- 5G/Edge security for mobility
- Secure message signing and verification
  Case Study: V2X cooperative-driving disruption due to falsified safety messages.

Module 4: Threat Modeling & Risk Assessment

- HEAVENS 2.0 methodology
- EVITA security architecture
- Defining assets, threats, and attack paths
- Risk scoring and prioritization
- Security controls selection
  Case Study: Threat modeling of an ADAS lane-assist subsystem.

Module 5: Autonomous Driving System Security

- AI/ML security vulnerabilities
- Sensor fusion integrity
- Adversarial attacks on perception systems
- Autonomous decision-making safety concerns
- Redundancy and fail-safe mechanisms
  Case Study: Adversarial stop-sign attack causing misclassification in autonomous vehicles.

Module 6: Secure Software, Firmware & OTA Updates

- Secure boot and firmware verification
- Cryptographic signing and hashing
- OTA update lifecycle and validation
- Cloud-to-vehicle update integrity
- Secure diagnostics and remote services
  Case Study: Unauthorized firmware injection on an ECU via insecure OTA pipeline.

Module 7: Automotive Penetration Testing & Validation

- Automotive pentesting methodologies
- In-vehicle network exploitation demos

- Hardware attack tools (JTAG, UART, SPI)
- Fuzzing for protocol vulnerabilities
- Reporting and mitigation frameworks
  Case Study: CAN bus injection enabling unauthorized control of vehicle subsystems.

Module 8: Incident Response, Monitoring & Cyber-Resilience

- Automotive SOC and security telemetry
- Real-time anomaly detection
- Incident response workflows for CAV fleets
- Digital forensics for vehicle systems
- Resilience engineering and recovery strategies
  Case Study: Fleet-wide telematics breach requiring coordinated incident response.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com