

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 21434SMV — Cybersecurity Engineering for Vehicles ISO SAE

ISO Certification Programme



LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference TR-SMV-21434SMV • ISO Transport

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	TR-SMV-21434SMV
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1 Advanced Cybersecurity Technologies 0 chapters85 marks	
2 Cybersecurity Risk Management 5 chapters · 30 classes85 marks	• 1 Fundamentals of Cybersecurity in Smart Vehicles — 6 classes › 1.1 Define Cybersecurity and Its Importance in Smart Vehicles › 1.2 Identify Common Cyber Threats and Vulnerabilities in Automotive Systems › 1.3 Explain the Role of Risk Management in Cybersecurity for Vehicles › 1.4 Assess Cybersecurity Risks in Smart Vehicle Environments › 1.5 Implement Basic Cybersecurity Measures for Vehicle Systems › 1.6 Evaluate Real-World Case Studies of Cybersecurity Breaches in Vehicles • 2 Risk Assessment Frameworks for Automotive Systems — 6 classes › 2.1 Define Key Concepts in Risk Assessment for Automotive Cybersecurity › 2.2 Identify Cybersecurity Threats Relevant to Automotive Systems › 2.3 Analyze Risk Assessment Frameworks Applicable to the Automotive Industry › 2.4 Evaluate Existing Risk Assessment Tools and Their Effectiveness › 2.5 Develop a Risk Assessment Plan Tailored for Automotive Applications › 2.6 Implement Risk Mitigation Strategies for Identified Vulnerabilities • 3 Implementing Risk Management Strategies in Vehicle Design — 6 classes › 3.1 Identify Key Cybersecurity Risks in Vehicle Design › 3.2 Assess Vulnerabilities within Vehicle Systems › 3.3 Develop Risk Mitigation Strategies for Identified Risks › 3.4 Implement Cybersecurity Controls in Vehicle Architecture › 3.5 Monitor and Evaluate Risk Management Effectiveness › 3.6 Integrate Continuous Improvement in Cybersecurity Practices • 4 Monitoring and Maintaining Cybersecurity Postures — 6 classes › 4.1 Assess Current Cybersecurity Postures in Vehicles › 4.2 Identify Key Metrics for Cybersecurity Monitoring › 4.3 Implement Continuous Monitoring Tools and Techniques › 4.4 Analyze Cybersecurity Incidents and Breaches › 4.5 Develop an Incident Response Plan for Vehicle Cybersecurity › 4.6 Review and Update Cybersecurity Policies and Procedures • 5 Incident Response and Recovery in Smart Vehicle Systems — 6 classes › 5.1 Identify Common Cybersecurity Incidents in Smart Vehicles › 5.2 Analyze Incident Response Frameworks for Automotive Systems › 5.3 Develop an Incident Response Plan for Smart Vehicle Systems › 5.4 Implement Communication Strategies During Cybersecurity Incidents › 5.5 Evaluate Recovery Techniques Post-Incident in Vehicle Systems › 5.6 Conduct a Simulation Exercise for Incident Response and Recovery
3 Designing Secure Vehicle Architectures 0 chapters65 marks	

• 1 Understanding Cybersecurity Incidents in Smart Vehicles — 6

classes

- › 1.1 Identify Common Cybersecurity Threats in Smart Vehicles
- › 1.2 Analyze Real-World Cybersecurity Incidents in the Automotive Sector
- › 1.3 Evaluate the Impact of Cybersecurity Incidents on Vehicle Safety
- › 1.4 Develop Incident Response Plans for Smart Vehicle Scenarios
- › 1.5 Implement Recovery Strategies Following Cybersecurity Breaches in Vehicles
- › 1.6 Conduct Post-Incident Reviews to Enhance Cybersecurity Preparedness

• 2 Incident Response Frameworks and Methodologies — 6 classes

- › 2.1 Identify Key Components of an Incident Response Framework
- › 2.2 Analyze Different Incident Response Methodologies
- › 2.3 Assess Risk Management Strategies in Cybersecurity
- › 2.4 Develop a Step-by-Step Incident Response Plan
- › 2.5 Implement Communication Protocols During an Incident
- › 2.6 Evaluate Recovery Strategies Post-Incident Analysis

• 3 Implementing Effective Incident Detection Mechanisms**• 4 Response Strategies for Cybersecurity Incidents****• 5 Recovery Planning and Post-Incident Analysis****• 1 Understanding ISO 21434: Key Principles and Definitions — 6**

classes

- › 1.1 Identify the Purpose of ISO 21434 in Automotive Cybersecurity
- › 1.2 Define Key Terminology Associated with ISO 21434 Standards
- › 1.3 Explain the Scope and Objectives of ISO 21434 Compliance
- › 1.4 Analyze the Structure and Components of ISO 21434 Framework
- › 1.5 Explore the Roles and Responsibilities within ISO 21434 Implementation
- › 1.6 Apply ISO 21434 Principles to Real-World Automotive Scenarios

• 2 Framework of Cybersecurity Risk Management in Vehicles — 6

classes

- › 2.1 Understand the Importance of Cybersecurity in Vehicle Engineering
- › 2.2 Identify Key Components of ISO 21434 Cybersecurity Risk Management Framework
- › 2.3 Analyze Cybersecurity Threats Specific to Vehicle Systems
- › 2.4 Assess Risk Assessment Methodologies for Vehicle Cybersecurity
- › 2.5 Develop a Cybersecurity Risk Management Plan for Vehicles
- › 2.6 Implement Continuous Monitoring and Improvement Strategies in Vehicle Cybersecurity

• 3 Cybersecurity Lifecycle: Planning and Development Processes —

6 classes

- › 3.1 Identify Key Stages of the Cybersecurity Lifecycle
- › 3.2 Define Goals and Objectives for Cybersecurity Planning
- › 3.3 Assess Risks and Vulnerabilities in Vehicle Systems
- › 3.4 Develop a Cybersecurity Framework for Vehicle Systems
- › 3.5 Implement Security Controls and Mitigation Strategies
- › 3.6 Evaluate and Monitor Cybersecurity Performance in Development

• 4 Implementation of Security Controls: Technical and Managerial Aspects — 6 classes

- › 4.1 Identify Key Technical Security Controls in ISO 21434
- › 4.2 Assess Risks and Threats During Vehicle Cybersecurity Implementation
- › 4.3 Develop a Management Framework for Cybersecurity in Vehicles
- › 4.4 Evaluate Compliance Requirements for Security Controls
- › 4.5 Integrate Security Controls into Vehicle Development Processes
- › 4.6 Create an Action Plan for Continuous Improvement of Cybersecurity Measures

• 5 Compliance Audits and Continuous Improvement in Cybersecurity Engineering — 6 classes

- › 5.1 Understand the Importance of Compliance Audits in Cybersecurity Engineering
- › 5.2 Identify Key Components of the ISO 21434 Compliance Audit Process
- › 5.3 Analyze Common Non-Conformities in Cybersecurity Engineering Audits
- › 5.4 Develop Strategies for Effective Audit Preparation and Execution
- › 5.5 Implement Processes for Continuous Improvement Post-Audit
- › 5.6 Evaluate the Impact of Continuous Improvement on Cybersecurity Practices