

WM9QP-15 Automotive Cyber Security

26/27

Department

WMG

Level

Taught Postgraduate Level

Module leader

Christo Panchev

Credit value

15

Module duration

4 weeks

Assessment

Multiple

Study location

University of Warwick main campus, Coventry

Description

Introductory description

This module explores the intersection between automotive technology and cybersecurity. The core principles of safeguarding modern vehicles against cyber threats will be explored, covering industry-standard protocols, security infrastructure, and methods for secure communication. Emphasis is placed on real-world applications, allowing students to learn about the cyber security measures implemented in the automotive sector and to confront the challenges faced by industry professionals in this rapidly evolving field.

Module aims

The module aims to instil students with a thorough understanding of automotive cyber security principles. Foundational concepts will enable them to analyse and comprehend vehicle architectures, communication networks, and associated security measures. Advanced topics will involve identifying attack surfaces and vulnerabilities, in inter and intra-vehicle communication interfaces and Over-the-Air (OTA) updates. Additionally, students will be introduced to industry-standard platforms like AUTOSAR Classic and Adaptive and learn how cryptographic operations contribute to securing vehicle systems. Lastly, students will engage with cyber security standards and risk assessment methodologies designed for the automotive sector, develop skills in threat modelling, and understand the functionality of intrusion detection systems in an automotive context. By the end of the module, students will be well-prepared to contribute to the exciting and

specialised field of automotive cyber security.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

- Overview of vehicle architectures and types of ECUs
- Networks in vehicles including CAN, CAN FD, Ethernet, LIN
- Communication interfaces: intra-vehicle and inter-vehicle, and challenges of increased connectivity
- Exploring attack surfaces and vulnerabilities
- Security infrastructure and key management to secure vehicle communications
- Introduction to the AUTOSAR Classic and Adaptive platform
- Cryptographic operations within the AUTOSAR framework
- Role of OTA updates in automotive systems for maintaining security, performance, and functionality of modern vehicles
- Security requirements for OTA updates including protection against Denial of Service (DoS) attacks and rollback mechanisms
- Introduction to UNECE R155/R156 and ISO/SAE 21434 cyber security standards for automotive
- Using risk assessment methodologies such as the NIST Cybersecurity Framework and ISO/SAE PAS 8475 guidelines
- Application of threat modelling using attack trees, STRIDE, and DREAD methodologies
- Introduction to intrusion detection and types of intrusion detection systems in an automotive context
- Exploring emerging intrusion detection mechanisms

Learning outcomes

By the end of the module, students should be able to:

- Evaluate the fundamental automotive cyber security concepts, including vehicle architectures, communication networks, and the challenges of increased connectivity.
- Identify and analyse attack surfaces, vulnerabilities, and potential cyber threats in automotive systems, and provide appropriate security measures to mitigate them.
- Evaluate and apply industry-standard methods in risk assessments and threat modelling using. Analyse and assess cyber security and safety standards and frameworks relevant to the automotive industry, such as UNECE R155/R156 and ISO/SAE 21434.
- Develop a discerning perspective on the design and engineering of security measures, such as intrusion detection systems, cryptographic operations, and secure OTA update mechanisms, to safeguard automotive systems against cyber-attacks.

Indicative reading list

[Reading lists can be found in Talis](#)

Research element

There is a strong emphasis on the development, growth and enhancement of individual research skills so as to provide participants with the high level research knowledge, skills and competencies needed to undertake an independent, original piece of research. The module content draws upon and highlights research within the domain and the module assessment requires participants to perform further research before preparing a response to the assessment task.

Subject specific skills

Experience in both practical application and theoretical understanding of automotive cyber security concepts.

Mastery of vehicle architectures, networks, and communication interfaces, coupled with adept awareness of cyber security threats

Understanding of the AUTOSAR software standardisation for the automotive industry

Understanding how the functionality of modern vehicles is maintained and enhanced through secure updates

Experience in applying risk assessment, threat modelling, and intrusion detection in an automotive context.

Transferable skills

Teamwork; Research and analysis; Report writing and scientific communication; Data collection; Critical thinking and problem solving

Study

Study time

Type	Required
Supervised practical classes	30 sessions of 1 hour (33%)
Online learning (independent)	10 sessions of 1 hour (11%)
Private study	50 hours (56%)
Total	90 hours

Private study description

Further practical lab work and research.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time	Eligible for self-certification
Analysis and reflection on experimental results A report presenting evidence backed critical analysis of results from lab work.	30%	15 hours	Yes (extension)
Risk assessment and securing an automotive system A report on performing a risk assessment and securing an automotive system from given specification. The assessment includes a practical element where based on the results from the risk assessment, students will be expected to secure the provide automotive system.	70%	45 hours	Yes (extension)

Assessment group R1

	Weighting	Study time	Eligible for self-certification
Analysis and reflection on experimental results	30%		No
Risk assessment and securing an automotive system A report presenting evidence backed critical analysis of results from lab work.	70%		No

Feedback on assessment

Feedback will be provided on a standard WMG feedback form.

Availability

Courses

This module is Optional for:

- Year 1 of TWMS-H1S1 Postgraduate Taught Cyber Security Engineering (Full-time)
- Year 1 of TWMS-H1SH Postgraduate Taught Cyber Security Management (Full-time)