Course guide
240273 - 240AU130 - Telematics

Last modified: 16/05/2023

Unit in charge: Barcelona School of Industrial Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: MASTER'S DEGREE IN INDUSTRIAL ENGINEERING (Syllabus 2014). (Optional subject).
MASTER'S DEGREE IN AUTOMOTIVE ENGINEERING (Syllabus 2019). (Optional subject).

Academic year: 2023 **ECTS Credits:** 6.0 **Languages:** Spanish

LECTURER

Coordinating lecturer: Francisco José Rico Novella

Others: Josep Paradells Aspas

REQUIREMENTS

The course is based on the knowledge about communication systems already seen in previous courses, and goes into detail on specific systems for the automotive industry

TEACHING METHODOLOGY

Lectures
Application classes
Individual work (non-presential)
Group work (non-presential)
Short response tests (control)
Short answer tests (test)
Long Answer Tests (Final Exam)

LEARNING OBJECTIVES OF THE SUBJECT

The course is divided into two parts that are taught in parallel, but in a coordinated manner, since the knowledge offered in each part is reused by the other.

One part aims to describe the communications used in the vehicles, including internal (communication buses) and external communications (driver, other vehicles and service platforms). The latter can be bi-directional such as those relating to access to information, or unidirectional such as those used by GNSS (Global Navigation Satellite System) systems for location purposes.
These communications have different requirements such as delay or speed, but mainly safety. Communications should be prevented from being inspected (privacy violation) or altered in such a way that the physical safety of the passengers or the vehicle itself may be compromised. Given the importance of security, the other part of the course is dedicated to this topic. Knowledge of communication security mechanisms and techniques are provided.
The course combines a theoretical and a practical part, both dedicated to study the communication systems and their security. The course is based on the knowledge about communication systems already seen in previous courses, and goes into detail on specific systems for the automotive industry. In the same way, safety concepts are introduced and exemplified in automotive communications. There are two types of classes: theoretical and application. In the first ones, the basic principles are presented and in the second ones, the knowledge is particularized to real automotive use, with the opportunity to visualize this knowledge in demonstration classes or by means of exercises.

STUDY LOAD

Type	Hours	Percentage
Self study	96,0	64.00
Hours small group	54,0	36.00

Total learning time: 150 h

CONTENTS

Security part (Theory: 19 h, Application: 6, Autonomous learning: 48h)

Description:
1. Introduction to cryptography (Theory: 2h. Autonomous learning: 4h)
Security Services
Classic vs. modern cryptography
2. Symmetric key cryptography (Theory: 5h + 1h Application. Autonomous learning: 8h)
Stream ciphers
Block ciphers
Encryption modes
Applications
3. Public key cryptography (Theory: 8h + 3h Application. Autonomous learning: 21h)
Definitions
Complexity theory
Diffie-Hellman
RSA
Other encryption methods
Digital Signature
Elliptic curve cryptography
Implications of Quantum Computing
4. Tamperproof systems (Theory: 2h. Autonomous learning: 4h)
Application to the security element
5. Examples in automotive (Theory: 4h + 2h Application. Autonomous learning: 11h)
Jamming and spoofing
Security algorithms in RFID: Crypto1
Rooling Codes
Relay attack
Use of certificates in vehicular communications

Full-or-part-time: 25h
Theory classes: 25h

In-vehicle communication part (Theory: 20h, Application: 5h, Autonomous learning: 48)

Description:
1. Services that require connection in a vehicle (Theory: 2h. Autonomous learning: 4h)
Maintenance
Location
Access
Saving on cable
Safe driving
Information and entertainment
Remote steering
2. Satellite based location services (Theory: 2h. Autonomous learning: 4h)
GNSS Systems
Assistance
3. Mobile phone connection with the vehicle (Theory: 4h + Application 2h. Autonomous learning: 10h)
Bluetooth
Profiles
Platforms (Google Android Auto, Apple CarPlay and MirrorLink)
4. Access to the vehicle (Theory: 4h + Application 2h. Autonomous learning:8h)
Digital keys
Immobilizer
RFID
Wireless keys
Access Control
Wake-up systems
Location system
5. Saving cable (Theory: 1h. Autonomous learning: 2h)
Tyre pressure monitoring
6. Cellular systems (Theory: 3h + Application 1h. Autonomous learning: 8h)
4G and 5G
eCall
7. Vehicle to vehicle communications (Theory: 4h Autonomous learning: 12h)
IEEE802.11p
C-V2X
Protocol architectures

Full-or-part-time: 25h
Theory classes: 25h

GRADING SYSTEM

BIBLIOGRAPHY

Basic:
- Held, Gilbert. Inter- and Intra-Vehicle communications [on line]. Boca Raton: CRC Press, 2008 [Consultation: 21/10/2022]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=321835. ISBN 9780367388317.
- Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan. "Cybersecurity challenges in vehicular communications". Vehicular Communications [on line]. Volume 23, 2020, ISSN 2214-2096 [Consultation: 17/07/2020]. Available on: https://www-sciencedirect-com.recursos.biblioteca.upc.edu/journal/vehicular-communications.- Lucena López, Manuel. Criptografía y seguridad en computadores [on line]. 5a ed. s.l.: s.n., 2022 [Consultation: 21/04/2023]. Available on: https://ccia.esei.uvigo.es/docencia/SSI/cripto.pdf.

Complementary:

- Menezes, A. J. ; Scott A. Vanstone ; Paul C. Van Oorschot. Handbook of applied cryptography. Boca Ratón [etc.]: CRC Press, cop. 1997. ISBN 0849385237.
- Verdult, R.; Garcia, Flavio D.; Balasch, J. "Gone in 360 Seconds: Hijacking with Hitag2". 21st USENIX Security Symposium (USENIX Security 2012) [on line]. [Consultation: 26/04/2023]. Available on: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf.