Module Name: (B.1) Security and Privacy in Cyberphysical Systems

Aim

This module aims to provide students with extensive knowledge and skills to make a holistic approach on identifying and satisfying security and privacy requirements for cyberphysical systems, the driving force of modern culture and an integral part of critical infrastructures, industrial systems, smart cities and transportation, agriculture, smart homes, e-health and more.

Learning Objectives

The learning objectives include the thorough understanding and analysis of the threats and security and privacy challenges and requirements for the protection of cyberphysical systems. This will be done in conjunction with the study of the attack surface on such systems, which formally allows attackers to exploit possible vulnerabilities in communications, the devices themselves and in data management processes. The study of standardized information security management methodologies and of the applicable legal framework will provide the means to approach the issue in a systematic manner. By participating in case studies that will be analyzed during this course, participants will be able to identify the threats and security measures of information and privacy-preserving solutions that can be deployed to shield these systems in various application domains.

Learning Outcomes

On successful completion of this module, students should be able to:

- Analyze scientific research papers and describe the role of cyberphysical systems and their needs from a security perspective.
- Analyze security and privacy requirements for various deployment environments.
- Analyze threats and vulnerabilities and methods that can be used by a threat agents to deploy an attack.
- Apply standardized information security management methods that can be used to secure information systems.
- Identify privacy issues and propose privacy-preserving solutions that can efficiently address them.
- Familiarize with open source platforms used for the management of cyberphysical systems and their data

Bibliography

[1] Alcaraz, C., Security and privacy trends in the industrial internet of things. Springer, 2019. https://doi.org/10.1007/978-3-030-12330-7

[2] S. Ziegler, Internet of Things Security and Data Protection, Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-04984-3

[3] Refsdal, B. Solhaug, and K. Stølen. Cyber-Risk Management. Springer, 2015. https://doi.org/10.1007/978-3-319-23570-7