

WM3F1-15 Cyber-Physical Systems

27/28

Department

WMG

Level

Undergraduate Level 3

Module leader

Christo Panchev

Credit value

15

Module duration

10 weeks

Assessment

100% coursework

Study location

University of Warwick main campus, Coventry

Description

Introductory description

Much attention relating to cyber security is focussed on the digital aspects of cyber systems; all data tends to be represented as pure, abstract, ones and zeros. In reality, all these abstract ones and zeros need a physical representation in order to have an effect. That physical representation might be as electromagnetic radiation, travelling through space as a radio wave, it might be as electric charge in an electronic device or it could take a range of other forms.

Control systems gather information from a range of physical sensors (flow rate sensors, temperature gauges, accelerometers etc); after processing, they generate outputs which in turn produce physical effects via actuators (switches, motors, displays etc).

Much attention relating to communication in the cyber domain is focussed around the Internet. A range of other communication protocols and technologies are widely deployed in industrial control, vehicle and other systems.

Understanding the significant characteristics of the physical manifestations of digital information, understanding the interconnectedness of the cyber domain with the physical domain via sensors and actuators, and understanding non-Internet technologies and protocols reduces the risk of inadvertently leaving a cyber system in a vulnerable position.

The overall aim of this module is to enable the cyber security specialist to have a meaningful conversation with practising engineers concerning the security of cyber-physical systems.

Module aims

To acquaint students with the particular cyber security issues surrounding cyber-physical systems.

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.

Operational technology (OT) and SCADA/ICS control systems

Security Architecture and Engineering for OT Systems

Vulnerability Management for OT systems

Cyber threat Intelligence for OT systems

Security Risk Management for OT systems

Learning outcomes

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

- Analyse the cyber security characteristics of selected cyber-physical technologies. (AHEP4 2.1.1, 2.1.5, 2.1.6, 2.1.10, 2.1.11, 2.2.2, C12)
- Analyse the significant cyber security characteristics of selected cyber-physical protocols. (AHEP4 2.1.1, 2.1.5, 2.1.6, 2.1.10, 2.1.11, 2.2.2, C12)
- Critically evaluate the cyber security constraints in selected cyber-physical domains. (AHEP4 2.1.1, 2.1.5, 2.1.6, 2.1.10, 2.1.11, 2.2.2, 2.3.2, C12)
- Design effective security controls in protecting cyber-physical systems. (AHEP4 2.1.2, 2.1.5, 2.1.8, 2.1.12, 2.2.1, 2.2.6, C10, C13)

Indicative reading list

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

Subject specific skills

Critically understand the differences between the cyber security requirements of conventional IT systems, and those of cyber physical systems.

Analyse the cyber security requirement of a cyber-physical system

Secure design of cyber-physical systems

Transferable skills

Critical and analytical thinking, problem solving

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Supervised practical classes	20 sessions of 1 hour (13%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Additional 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 A

	Weighting	Study time	Eligible for self-certification
Assessment component			
In-class test	30%	18 hours	No
An online test with a combination of multiple choice and short answer questions.			

Reassessment component is the same

Assessment component			
Coursework	70%	42 hours	Yes (extension)
A report outlining the results of an investigation into a cyber physical system related problem/challenge			

Weighting**Study time****Eligible for self-certification****Reassessment component**

Coursework

No

A report outlining the results of an investigation into a cyber physical system related problem/challenge

Feedback on assessment

Written feedback provided with the mark via tabula.

Availability**Courses**

This module is Core optional for:

- UWMA-H651 Undergraduate Cyber Security
 - Year 3 of H651 Cyber Security
 - Year 3 of H651 Cyber Security
 - Year 3 of H651 Cyber Security