WM240-24 The Cyber Context of Software Engineering

21/22

Department
WMG
Level
Undergraduate Level 2
Module leader
Tony Green
Credit value
24
Module duration
30 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

Software engineering is the discipline concerned with the application of theory, knowledge, and practice to effectively and efficiently build reliable software systems that satisfy the requirements of customers and users. This discipline is applicable to small, medium, and large-scale systems. It encompasses all phases of the lifecycle of a software system, including requirements elicitation, analysis and specification; design; construction; verification and validation; deployment; and operation and maintenance. Whether small or large, following a traditional plan-driven development process, an agile approach, or some other method, software engineering is concerned with the best way to build good software systems. This module will look at software engineering in the context of cyber security, applying frameworks such as Trustworthy Software Framework when developing software systems.

Module aims

1 – Apply cyber security good practice to various phases of the software engineering lifecycle.

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.

Outline content
The content of this module will be taught from a cyber security perspective.

- software processes
- software project management
- tools and environments to support and manage:
- requirements engineering
- software design
- software construction
- software verification and validation
- software evolution in the context of large, pre-existing code bases
- software reliability
- secure software development

Learning outcomes

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

- 1 – Apply cyber security good practice to various phases of the software engineering lifecycle.
- 2 - Participate in a team, engaged in a project at some phase of the software engineering lifecycle.

Indicative reading list

Merkow, Mark S. and Raghavan, Lakshmikanth, “Secure and Resilient Software Development”, Auerbach Publications (2010)

Sommerville, Ian, "Software Engineering", 10 Ed, Pearson (2015)

Whittaker, James A., “Exploratory Software Testing”, Addison-Wesley (2009)

Subject specific skills

1 – Apply cyber security good practice to various phases of the software engineering lifecycle.
2 - Participate in a team, engaged in a project at some phase of the software engineering lifecycle.

Transferable skills

Teamwork, problem solving

Study

Study time

Type	Required
Supervised practical classes	18 sessions of 2 hours 30 minutes (19%)
Private study	65 hours (27%)
Assessment	130 hours (54%)
Total	240 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A3

	Weighting	Study time
Portfolio	100%	130 hours

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions
Summative feedback on assignments

Availability

Pre-requisites

Can program competently in at least one language and thus able to learn to program in another language.

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security
  - Year 2 of H651 Cyber Security