



## MODULE SPECIFICATION

Part 1: Information			
Module Title	Internet of Things		
Module Code	UFCFDN-15-3	Level	Level 6
For implementation from	2020-21		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description
<p><b>Educational Aims:</b> The Internet of Things (IoT), is the connecting and internetworking of multiple devices over the internet, allowing them to communicate with us, applications, and each other. This module aims to provide apprentices with an in-depth appreciation of the Internet of Things (IoT). Delivery/research will cover modern system architecture, key technologies, and legal, social and ethical/moral implications to implementing these technologies.</p> <p><b>Outline Syllabus:</b> You will cover:</p> <ul style="list-style-type: none"> <li>System architecture (e.g. centralised and decentralised) (Component B) □</li> <li>Sensing technologies (e.g. sensors and actuators) (Component B) □ Machine-to-Machine (M2M)</li> <li>Communication (Component B) □ Wireless technologies (Component B)</li> <li>Messaging/communication protocols(Component B)</li> <li>Hardware and software platforms for IoT (Component A)</li> <li>Legal, social, ethical, and moral implications of IoT e.g. IoT security and privacy (Component A)</li> <li>Effective cyber security in relation to IoT (Component B)</li> <li>Data security and management with regards to IoT (Component A)</li> </ul> <p><b>Teaching and Learning Methods:</b> Introductory lectures are supported by seminars, case studies, visits and practical workshops. In addition this module will be supported by interactive</p>

## STUDENT AND ACADEMIC SERVICES

forums and learning tools.

150 hours study time of which 36 hours will represent scheduled learning. Scheduled learning includes lectures, seminars, tutorials, demonstration, practical classes and workshops; external visits; supervised time in studio/workshops.

Independent learning includes hours engaged with essential reading, case study preparation, assignment preparation and completion. Apprentice study time will be organised each week with a series of both essential and further readings and preparation for practical workshops. It is suggested that preparation for lectures, practical workshops, session delivery and seminars will take 7 hours per week.

Scheduled learning will typically include lectures, seminars, supervision, external visits and an interactive forum.

All apprentices are expected to attend a series of tutorials.

### Part 3: Assessment

Assessment 1 – Component A Apprentices will be required to prepare a 15 minutes presentation on the Legal, social, ethical, and moral implications of IoT e.g. IoT security and privacy. With reference the associated data and security management and the hardware and software platforms that may be adopted to meet the user requirements

Assessment 2 – Component B Apprentices are expected to produce a literature review on the Internet of Things (IoT). Apprentices should create a hypothesis or theory of research that enables them to analyse current IoT system architecture(s), critically review current IoT technologies, outline current IoT hardware and software platforms, and critically appraise the legal, social, ethical, and moral implications. It is suggested that apprentices agree their hypothesis with the module leader or subject lecturer.

First Sit Components	Final Assessment	Element weighting	Description
Presentation - Component A	✓	50 %	Presentation (15 mins)
Written Assignment - Component B		50 %	Literature review (3000 words)
Resit Components	Final Assessment	Element weighting	Description
Presentation - Component A	✓	50 %	Presentation (15 mins)
Written Assignment - Component B		50 %	Literature review (3000 words)

### Part 4: Teaching and Learning Methods

Learning Outcomes On successful completion of this module students will achieve the following learning outcomes:

Module Learning Outcomes	Reference
Analyse current IoT system architecture(s), demonstrating understanding of their key features.	MO1
Critically review current IoT technologies.	MO2
Outline current IoT hardware and software platforms.	MO3
Critically appraise the legal, social, ethical, and moral implications of IoT.	MO4

## STUDENT AND ACADEMIC SERVICES

	Analyse and evaluate security threats and vulnerabilities with regards to IoT and identify how these can be mitigated.	MO5
	Critically review the security implications that IoT could present in terms of corporate responsibility.	MO6
	Discuss the associated data implication that IoT could represent in the future, linking to legal, social and ethical/moral implications.	MO7
	Research and investigate common and emerging attack techniques with reference to IoT and recommend how to defend against them	MO8
	The range of data protection and current legal issues.	MO9
Contact Hours	<b>Independent Study Hours:</b>	
	Independent study/self-guided study	114
	<b>Total Independent Study Hours:</b>	114
	<b>Scheduled Learning and Teaching Hours:</b>	
	Face-to-face learning	36
	<b>Total Scheduled Learning and Teaching Hours:</b>	36
	<b>Hours to be allocated</b>	150
	<b>Allocated Hours</b>	150
Reading List	<p>The reading list for this module can be accessed via the following link:</p> <p><a href="https://uwe.rl.talis.com/modules/ufcfdn-15-3.html">https://uwe.rl.talis.com/modules/ufcfdn-15-3.html</a></p>	

### Part 5: Contributes Towards

This module contributes towards the following programmes of study: