



## **Module Specification**

### **Internet of Things (IoT)**

Version: 2023-24, v2.0, 16 Mar 2023

#### **Contents**

<b>Module Specification .....</b>	<b>1</b>
<b>Part 1: Information .....</b>	<b>2</b>
<b>Part 2: Description .....</b>	<b>2</b>
<b>Part 3: Teaching and learning methods .....</b>	<b>4</b>
<b>Part 4: Assessment.....</b>	<b>5</b>
<b>Part 5: Contributes towards .....</b>	<b>6</b>

## Part 1: Information

**Module title:** Internet of Things (IoT)

**Module code:** UFCFBR-30-3

**Level:** Level 6

**For implementation from:** 2023-24

**UWE credit rating:** 30

**ECTS credit rating:** 15

**Faculty:** Faculty of Environment & Technology

**Department:** FET Dept of Computer Sci & Creative Tech

**Partner institutions:** None

**Delivery locations:** Not in use for Modules

**Field:** Computer Science and Creative Technologies

**Module type:** Module

**Pre-requisites:** None

**Excluded combinations:** None

**Co-requisites:** None

**Continuing professional development:** No

**Professional, statutory or regulatory body requirements:** None

## Part 2: Description

**Overview:** 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.

**Features:** Not applicable

**Educational aims:** This module aims to provide learners with an in-depth appreciation of the Internet of Things (IoT) and the tools to design and develop their own multi-device IoT Solution to meet a project requirement.

In completion of this module learners should be able to:

Plan, develop and test a secure multi-client IoT solution to meet a defined scenario using suitable IoT enabled hardware and software. Software languages could include Windows IOT Core, Python.

Node/Node Red, C. Suitable IoT hardware devices:

Raspberry Pi

Arduino

BeagleBoard

Intel Edison

Google Coral

Evaluate different M2M protocols (eg technology, range, costs, bandwidth, regulation, limitations)

Use a variety of sensors to monitor, record data and trigger actions accordingly  
Provide clear and meaningful user access to sensors/data via a web accessible interface or dashboard hosted on a suitable web/cloud/IoT hosting platform.

Identify key legislation impacting the publication of IoT Solutions, eg Data Governance (IPO, GDPR, Data Protection), privacy policies, use of data etc.

**Outline syllabus:** Delivery will cover modern system architecture, key technologies, and legal, social and ethical/moral implications to implementing these technologies.

System architecture (e.g. centralised and decentralised)

Machine-to-Machine (M2M) Communication (e.g. Wireless technologies, Messaging/communication protocols)

Hardware and software platforms for IoT

Legal, social, ethical, and moral implications of IoT

Effective cyber security in relation to IoT

Students will be able to cultivate independent technical judgement in the use of techniques and tools associated with IoT devices and M2M communication

protocols. As well as being able to develop the ability to think conceptually and translate concepts into reality, learners will go beyond programming web applications, and develop skills in security, penetration testing and user experience.

### **Part 3: Teaching and learning methods**

**Teaching and learning methods:** Introductory lectures are supported by seminars, case studies, visits and practical workshops. In addition this module will be supported by interactive forums and learning tools. Students must have access to a suitable publicly accessible hosting platform and database server to be able to complete this module.

300 hours study time of which 108 hours will represent scheduled learning. Scheduled learning includes lectures, seminars, tutorials, demonstration, practical classes and workshops; external visits; supervised time in studio/workshop.

**Module Learning outcomes:** On successful completion of this module students will achieve the following learning outcomes.

**MO1** Explain common security risks present when building and publishing web driven IoT solutions and best practice authentication (e.g. injection protection, code injection/data validation, protection from brute force attacks, encryption techniques, end to end encryption).

**MO2** Evaluate key IoT hardware and software solutions

**MO3** Evaluate different M2M protocols

**MO4** Plan, develop and test a secure multi-client IoT solution to meet a defined scenario using suitable IoT enabled hardware and software.

**MO5** Use a variety of sensors to monitor, record data and trigger actions to empower a complete IoT solution

**MO6** Understand key legislation impacting the publication of IoT Solutions

**Hours to be allocated:** 300

**Contact hours:**

Independent study/self-guided study = 192 hours

Face-to-face learning = 108 hours

Total = 300

**Reading list:** The reading list for this module can be accessed at [readinglists.uwe.ac.uk](https://uwe.rl.talis.com/index.html) via the following link <https://uwe.rl.talis.com/index.html>

## **Part 4: Assessment**

**Assessment strategy:** This module is assessed by a combination of techniques: an examination and a practical portfolio.

Exam (includes the following):

Fundamentals of IoT technology (e.g. Hardware, software, sensors, frameworks)

Evaluate/compare different M2M protocols

Key legislation impacting the publication of IoT Solutions, e.g. Data Governance (IPO, GDPR, Data

Protection), privacy policies, use of data etc.

Practical Portfolio (includes the following):

Evidence of planning and design of a IoT solution to support an agreed scenario

Implementation of an IoT solution to support a scenario consisting of a minimum of two interconnected devices and a selection of suitable sensors.

Deploying and test a completed IoT solution

Documenting complete IoT solution

Opportunities for formative assessment exist for the assessment strategy used.

Verbal feedback is given and all students will engage with personalised tutorials setting SMART targets as part of the programme design.

### **Assessment components:**

#### **Examination (Online) (First Sit)**

Description: Online multiple choice exam (1.5 hours)

Weighting: 30 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO6

**Practical Skills Assessment (First Sit)**

Description: Practical Skills Assessment - Design, build, and test an IoT solution

Weighting: 70 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO4, MO5

**Practical Skills Assessment (Resit)**

Description: Practical Skills Assessment - Design, build, and test an IoT solution

Weighting: 70 %

Final assessment: Yes

Group work: No

Learning outcomes tested:

**Examination (Online) (Resit)**

Description: Online multiple choice exam (1.5 hours)

Weighting: 30 %

Final assessment: No

Group work: No

Learning outcomes tested:

**Part 5: Contributes towards**

This module contributes towards the following programmes of study:

Applied Computing[Sep][FT][UCW][3yrs] BSc (Hons) 2021-22

