



Module Specification

Critical Systems Security

Version: 2021-22, v2.0, 06 Oct 2021

Contents

Module Specification	1
Part 1: Information	2
Part 2: Description	2
Part 3: Teaching and learning methods	4
Part 4: Assessment.....	5
Part 5: Contributes towards	7

Part 1: Information

Module title: Critical Systems Security

Module code: UFCF7P-15-M

Level: Level 7

For implementation from: 2021-22

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Delivery locations: Frenchay Campus

Field: Computer Science and Creative Technologies

Module type: Standard

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Not applicable

Features: Not applicable

Educational aims: This module will introduce students to the cyber security threats and risks in Critical Systems, with a particular focus on Industrial Control Systems (ICS) and Supervisor Control and Data Acquisition (SCADA) systems. Students will

also examine conventional ICS cyber-protection methods and new security approaches proposed by the research community or adopted by the Industry, exploring the emerging challenges and limitations.

Outline syllabus: Introduction to Critical Systems:

Basic Terminology on CI and ICS components.

The evolution of ICS.

ICS as a system of systems and the emerging interdependencies.

ICS types and their components.

Comparison between IT and Critical Systems in the context of cyber security.

Cyber security threats in ICS:

Analysis of known case studies - the examples of Stuxnet, Duqu and Flame.

Other examples found in the literature.

Advanced Persistent Threats (APTs).

Analysis of attack vectors (the notions of cyber-terrorism, state-sponsored attacks and cyber-warfare).

Impact analysis (direct physical impact, physical disruption; systemic impact/ the domino effect).

Challenges and limitations of current cyber security approaches:

The risk of disruption (cyber security operational cost/ the cost of updating/upgrading systems).

Legacy and/or proprietary equipment and protocols (e.g. Modbus; Profibus, EtherCAT etc.).

Contemporary off-the-shelf equipment and protocols (the connection of ICS to the Internet).

Risk modelling and analysis:

Expert Elicited Models, Attack Graphs, Games, Petri Nets.

Measuring risks.

Situational awareness in ICS:

The kill chain process.

Sensors and data in ICS.

Governance and assessment of strategies:

Purpose of governance.

Governance in ICS

ISA 99/IEC 62443 (industrial automation and control systems security) and ISO/IEC 15408, ISO/IEC 27001:2015, ISO/IEC 27002:2013, ISO/IEC 27003:2010, ISO/IEC 27004:2009, ISO/IEC 27005:2011

Part 3: Teaching and learning methods

Teaching and learning methods: See Assessment

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

MO1 Demonstrate a deep and systematic understanding of conventional and contemporary ICS implementations and their comparison to IT systems in the context of cyber security On successful completion of this module students will achieve the following learning outcomes.

MO2 Undertake the analysis of the cyber threat landscape in ICS and evaluate current cyber protection approaches in the field On successful completion of this module students will achieve the following learning outcomes.

MO3 Design and evaluate improvements in current cyber protection approaches to tackle the cyber security challenges that arise in ICS On successful completion of this module students will achieve the following learning outcomes.

MO4 Select appropriate risk modelling methods in ICS and critically evaluate their effectiveness on risk measurement On successful completion of this module students will achieve the following learning outcomes.

MO5 Critically apply the Kill Chain process to model complex cyber security incident scenarios in ICS and develop situational awareness On successful completion of this module students will achieve the following learning outcomes.

MO6 Demonstrate an understanding of industry-specific regulations and standards for the protection of ICS

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at [readinglists.uwe.ac.uk](https://uwe.rl.talis.com/modules/ufcf7p-15-m.html) via the following link <https://uwe.rl.talis.com/modules/ufcf7p-15-m.html>

Part 4: Assessment

Assessment strategy: Component A: Written examination (2 hours). The examination will assess the students' knowledge and understanding of ICS implementations and their comparison to IT systems. It will assess the students' knowledge and understanding of the related industry-specific cyber security regulations and standards. It will also assess the students' ability to develop situational awareness, through the use of the Kill Chain process, on selected scenarios. Finally, it will assess the students' critical skills on the selection and evaluation of risk modelling methods to measure risks in specific tasks.

Component B: Written assignment / Report (2000 words) on cyber threat intelligence in ICS. Students will write a report analysing the current cyber threat landscape and cyber protection approaches in ICS and the challenges that arise in ICS implementations proposing improvements to address these challenges. The report will assess the students' understanding of ICS implementations, and their ability to analyse the relevant cyber threat landscape and evaluate current cyber security approaches. It will also assess their ability to design and evaluate improvements in current cyber security approaches. The student can draw information from past case

studies, including the case studies provided in the lectures (e.g. Stuxnet, Duqu, Flame), but they are required to use additional literature sources.

Assessment components:

Examination (Online) - Component A (First Sit)

Description: Online Written examination (2 hours)

24-hour window

Weighting: 50 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO4, MO5, MO6

Report - Component B (First Sit)

Description: Written assignment / report (2000 words) on a selected case study

Weighting: 50 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3

Examination (Online) - Component A (Resit)

Description: Online Written examination (2 hours)

24 hour window

Weighting: 50 %

Final assessment: Yes

Group work: No

Learning outcomes tested:

Report - Component B (Resit)

Description: Written assignment / report (2000 words) on a selected case study

Weighting: 50 %

Final assessment: No

Group work: No

Learning outcomes tested:

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Sep][FT][Frenchay][1yr] MSc 2021-22

Cyber Security [Sep][PT][Frenchay][2yrs] MSc 2020-21