MODULE DESCRIPTOR

Module Title

OT and ICS Security

Reference	CM4122	Version	2
Created	June 2022	SCQF Level	SCQF 10
Approved	May 2020	SCQF Points	15
Amended	July 2022	ECTS Points	7.5

Aims of Module

To provide students with the ability to identify cyber security threats and implement countermeasures within Operation Technology (OT) Networks and Industrial Control Systems (ICS).

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Identify and explain OT and ICS protocol vulnerabilities and evaluate the security of an industrial network infrastructure.
2	Design and implement countermeasures to protect an OT network and ICS from unauthorised access.
3	Understand the ethical, legal and operational policies of OT and ICS security testing.
4	Critically evaluate security controls used to protect OT and ICS networked systems.
5	Effectively communicate the results of OT and ICS auditing, assessing and security testing to demonstrate regulatory compliance.

Indicative Module Content

The ethical and legal issues relating to penetration testing OT and ICS. Network enumeration and network mapping. Use of network sniffers. OT and ICS device management and exploitation. Maintaining physical security of network devices. IoE security and wireless attacks. Best Practice Guides: ISO 27001, ISO 27005, ISO 27014, Cyber Assessment Framework, ISA99 and IEC 62443 (Series 2).

Module Delivery

This module is taught using a structured programme of lectures, lab sessions and student centred learning.

Module Ref:	CM4122 v2

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4, 5
Description:	An individual coursework assessment.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighing of C1. An overall minimum grade D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in C1.
B	The student needs to achieve a B in C1.
C	The student needs to achieve a C in C1.
D	The student needs to achieve a D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1	McNAB,C., 2016. Network Security Assessment. 3rd Ed. O'Reilly.
2	KIM, P., 2015. The Hacker Playbook 2: Practical Guide to Penetration Testing. CreateSpace Independent Publishing Platform.
3	WEIDMAN, G., 2014. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press
4	RADVANOVSKY, R. and BODSKY, J., 2016. Handbook of SCADA/Control Systems Security. 2nd Ed. CRC Press
5	HASSANIEN, A.E. and ELHOSENY, M., 2019. Cyber Security and Secure Information Systems: Challenges and Solutions in Smart Environments. ISBN: 978-3030168360