Title	Secure OT/ICS Networks
Long Title	Secure OT/ICS Networks
Credits	**6**
NFQ Level	9
Module Author	Muzaffar Rao

Module Description:

The aim of the module is to enable students to understand the differences between IT and OT security risks, the impacts of users behaviour and how to establish a Cyber Security Management System (CSMS). This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to the consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Assess, manage and evaluate Operational Technology (OT) Security.
LO2	Present mitigation strategies for OT security.
LO3	Identify the differences between Information Technology (IT) and OT security.
LO4	Develop a Cyber Security Management Strategy.
LO5	Value and accept the importance of security awareness for Operational Technology (OT).

Indicative Content

• **Cyber Threats, vulnerabilities and attack vectors**

o Importance of securing ICS. Threat landscape - Malware, exploits, APTs, insider threats, hacktivism, cybercrime, cyber terrorism, cyber war. Threat actors. Threat Intelligence and sharing. CIA triad. Vulnerabilities in ICS. Vulnerability assessment. Penetration testing. Vulnerability database. Common Vulnerability Scoring System (CVSS). Risk ranking - DREAD Model.

• **The OT concept of Asset/vulnerability management**

o Lots of legacy equipment, fear of IT intrusion etc.

• **ICS Security Architecture**

o Defence in Depth. Physical, Network, Computer, Application & Device Security. Security architecture for ICS. Security Architecture Patterns – access controls, network security, log management and remote access. Security Principles – Zones & Network Segmentation. establishing zones and conduits. Relationship of zones/conduits and Purdue Reference model. Zones and security device configuration.

• **Security Principles – Firewalls and Zoning**

o Network Segmentation. Zoning. Firewalls. Firewalls. Firewall configuration with zones. Access Control lists. VLANs. Host based Firewalls . Application based Firewalls

• **Security Principles – Intrusion Detection & Prevention**

o Network Intrusion Detection and Protection Systems. IDS/IPS recommendations for ICS.

• **Introduction to Security Monitoring**

o Security information and event management (SIEM). SIEM tools. SIEM data collection –firewalls, IDS/IPS, router and switch, OS and application logs. Achieving network visibility. Behavioural anomaly detection. Whitelist configuration. Event correlation.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written	Reflective journal summarizing and analysing the work carried out in weekly assigned labs.	1, 2, 3, 4, 5	30%	Due End of Sem
Practical	Lab based assessments	1, 2, 3, 4, 5	40%	Bi weekly
Written	Research report on the differences between IT and OT security.	1, 3, 5	30%	End of Sem

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Tutorial	Online support for student learning	1.0	Every Week	1.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	5.0	Every Week	5.0
		Total Hours		10
		Total Weekly Learner Workload		10
		Total Weekly Contact Hours		3.0

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Tutorial	Online support for student learning	1.0		1.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	5.0	Every Week	5.0
		Total Hours		10
		Total Weekly Learner Workload		10
		Total Weekly Contact Hours		3.0

Recommended Book Resources

- **Pascal Ackerman (2017) Industrial Cybersecurity: Efficiently secure critical infrastructuresystems, Packt Publishing**
- **Eric D. Knapp (Author), Joel Thomas Langill (Contributor). (2014) Industrial Network Security:Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial ControlSystems, Syngress Media, U.S.https://www.enisa.europa.eu/topics/standards**