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

Module Description:

The aim of the module is to provide knowledge, skills and abilities related to communication networks and protocols used in Operational Technology (OT), and the interconnections between them in Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA)systems. The module is aimed at helping students to better understand them and be prepared to integrate the systems into IT systems. 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	Evaluate network architectures and protocols used for Industrial Control Systems (ICS)
LO2	Evaluate and assess the interdependencies that can be found in ICS/Supervisory Control and Data Acquisition (SCADA) networks
LO3	Recommend the most suitable standard industrial communication protocol for an application.
LO4	Demonstrate an understanding of good practices in ICS networking.
LO5	Value and accept the importance of good practices that promote security in Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems.

Indicative Content

- **Industrial control systems**

ICS architecture – PLC, HMI, SCADA, DCS, SIS. ICS functions – view, monitor and control. Purdue Model for ICS. ICS zones and levels, enterprise, industrial demilitarized, and industrial zones.

- **ICS Media and Protocols**

Regular IT Network Protocols -HTTP, HTTPS, DNS, SMTP, FTP, SNMP, DHCP etc. Process Automation Protocols – Profibus, DeviceNet, ControlNet, Modbus, CIP. ICS Protocols – OLE for Process Control (OPC). OPC Unified Architecture. Building Automation Protocols – BACnet, C-Bus, Modbus, Zigbee, Z-Wave. Communication protocols mapped to different zones. AMI and the smart grid. Industrial Protocol Simulators for Modbus, DNP, OPC etc. Ethernet/IP and CIP. Availability and Resilience - Resilient Ethernet Protocol, Media Redundancy Protocol.

- **ICS Network Topologies & Services**

Common Topologies – star, bus, mesh, wireless mesh, tree, ring, dual homing. Network Segmentation, VLANs, physical and logical segmentation. Network services – DNS, DHCP, IAMetc. Network tools – wire shark, SIEM

- **ICS Network Configuration**

Modbus Serial Slave and master. PROFINET – device roles, configuration, troubleshooting. Ethernet/Industrial Protocol (IP).

- **Current state of secure implementations of the OT network space**

Secure extensions of ProfiNet, Ethercat etc.

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, 4, 5	30%	Due End of Sem
Practical	Lab based assessments	1, 2, 3, 4, 5	40%	Bi weekly
Written	Research report on ICS communication networks and protocols topic	1, 2, 4, 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**