PGDip / MSc
in

Industrial Cybersecurity and Critical Infrastructure

Overview

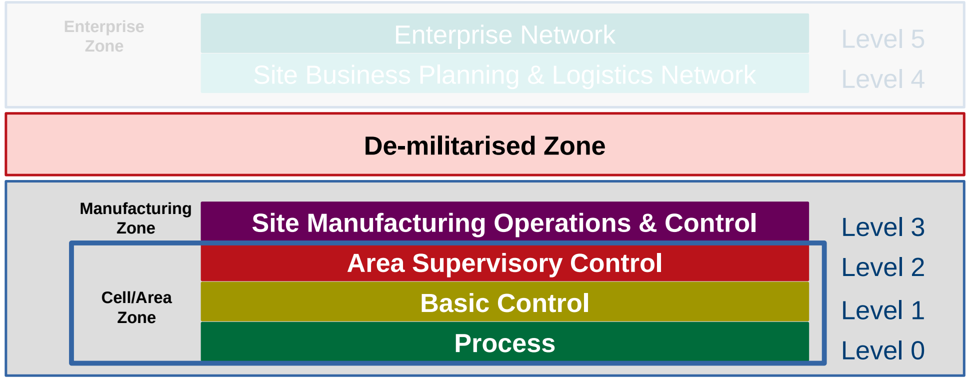
Qualification:	**PG Dip** in Industrial Cybersecurity and Critical Infrastructure
Award Type:	NFQ Level 9
Schedule:	1 Academic Year Full-time (September - May)

Qualification:	**MSc** in Industrial Cybersecurity and Critical Infrastructure
Award Type:	NFQ Level 9
Schedule:	1 Year Full-time (September - September)

Overview

- Requirements for admittance to programme
  - A relevant level 8 degree
  - A relevant level 7 degree with sufficient relevant industrial experience

Area of Interest



Enterprise Zone

Network	Level
Enterprise Network	Level 5
Site Business Planning & Logistics Network	Level 4

De-militarised Zone

Manufacturing Zone

Site Manufacturing Operations & Control	Level 3

Cell/Area Zone

Area Supervisory Control	Level 2
Basic Control	Level 1
Process	Level 0

Master of Science programme structure

Semester 1 (Sep-Dec)	Semester 2 (Jan-Apr)
Industrial Control Systems	Advanced Industrial Automation
Programming I	Programming II
Industrial Networks I	Industrial Networks II
Foundations, Structures and, Controls of Cybersecurity	Operational Technology (OT) Security and Architecture
Research Methods for Engineering	

Work-based Project and Professional Development 1&2 Sep-Apr

Dissertation Full year Sep-Sep

stephen.scully@setu.ie
Dr Stephen Scully

james.garland@setu.ie
Dr James Garland

keith.smyth@setu.ie
Mr Keith Smyth

dermot.farrelly@setu.ie
Mr Dermot Farrelly

edmond.tobin@setu.ie
Dr Ned Tobin

claire.odonoghue@setu.ie
Ms Claire O'Donoghue

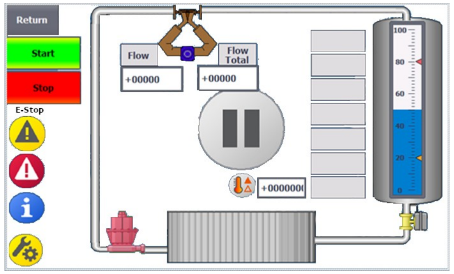
Indicative Timetable

	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000
Monday				Prog I (JG) C305		Cyber Security I (DF) A310		Research Methods (ET) C238	Cyber Security I (DF) C229				
Tuesday													
Wednesday			Research Methods (NT) C238			Cyber Security I (DF) C229		Industrial Net I (KS) C243					
Thursday		ICS (SS) C175				Industrial Net I (KS) D417		Prog I (JG) D505	Industrial Net I (KS) D505	WBL (COD)			
Friday				ICS (SS) C172		Industrial Net I (KS) A200	ICS (SS) J108						

Onsite

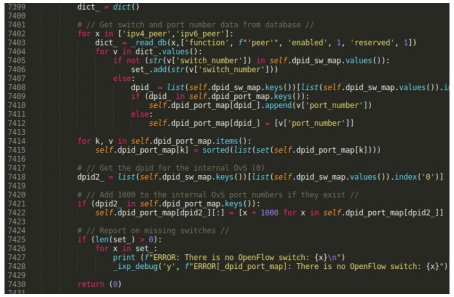
Online

Industrial Control Systems
Advanced Industrial Automation



Programming I and II

- Python Language
- Object Oriented Programming
- Networking Python
- Network Automation
- Automation Framework
- RESTful API
- Network Reconnaissance
- Capstone Project



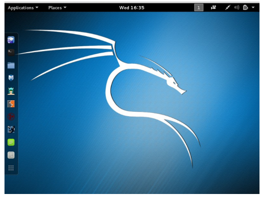
```python
        dict_ = dict()

        # // Get switch and port number data from database //
        for x in ['ipv4_peer','ipv6_peer']:
            dict_ = _read_db(x,['function', f"'peer'", 'enabled', 1, 'reserved', 1])
            for v in dict_.values():
                if not (str(v['switch_number']) in self.dpid_sw_map.values()):
                    set_.add(str(v['switch_number']))
                else:
                    dpid_ = list(self.dpid_sw_map.keys())[list(self.dpid_sw_map.values()).i
                    if (dpid_ in self.dpid_port_map.keys()):
                        self.dpid_port_map[dpid_].append(v['port_number'])
                    else:
                        self.dpid_port_map[dpid_] = [v['port_number']]

        for k, v in self.dpid_port_map.items():
            self.dpid_port_map[k] = sorted(list(set(self.dpid_port_map[k])))

        # // Get the dpid for the internal OvS (0)
        dpid2_ = list(self.dpid_sw_map.keys())[list(self.dpid_sw_map.values()).index('0')]

        # // Add 1000 to the internal OvS port numbers if they exist //
        if (dpid2_ in self.dpid_port_map.keys()):
            self.dpid_port_map[dpid2_][:] = [x + 1000 for x in self.dpid_port_map[dpid2_]]

        # // Report on missing switches //
        if (len(set_) > 0):
            for x in set_:
                print (f"ERROR: There is no OpenFlow switch: {x}\n")
                _ixp_debug('y', f"ERROR[_dpid_port_map]: There is no OpenFlow switch: {x}")

        return (0)
```

Industrial Networks I & II

- Compare enterprise and industrial ethernet
- IPv4 and IPv6
- Verify correct operation & fault find on IACS networks
- Network protocols, problem solving, security and communications
- IEEE 802.11x

Foundations, Structures and Controls of Cybersecurity Operational Technology (OT) Security and Architecture

- OT cybersecurity (OTSec) threat models
- OTSec Management solutions
- Implement holistic models based on international standards
- Meet EU and national legislation to ensure compliance and best practice
- Motivations, methodologies, risk and vulnerability assessment for OTSec
- Develop Incident Response Plans for OT environments
- Table-top immersion exercises.



Work-based Project & Professional Development
Ms Claire O'Donoghue

- Critically review and analyse a complex problem and develop a solution with consideration to business, commercial and ethical requirements.
- Plan, design and implement a project from initial problem definition to the presentation of results.
- Critically evaluate relevant data and information from a variety of sources and draw relevant conclusions.
- Develop and present a business case for a technical solution within a work-based environment.
- Demonstrate professional self-awareness, reflection, develop a professional development plan and apply professional skills to the acquisition of suitable employment.

Research methods and the dissertation

- Research methods module is a pre-requisite for being eligible to commence the dissertation.
- Presentations x 2 throughout semester 2.
- Viva will be required after submission of dissertation. You will need to defend your submission.