



## MODULE SPECIFICATION

Part 1: Information			
Module Title	Critical Systems Security		
Module Code	UFCF7P-15-M	Level	Level 7
For implementation from	2018-19		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Contributes towards	Cyber Security [Sep][FT][Frenchay][1yr] MSc 2018-19		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description
<p><b>Educational Aims:</b> 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.</p> <p><b>Outline Syllabus:</b> 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.</p> <p>Comparison between IT and Critical Systems in the context of cyber security.</p>

## STUDENT AND ACADEMIC SERVICES

<p>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).</p> <p>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).</p> <p>Risk modelling and analysis:          Expert Elicited Models, Attack Graphs, Games, Petri Nets.          Measuring risks.</p> <p>Situational awareness in ICS:          The kill chain process.          Sensors and data in ICS.</p> <p>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/27002:2013, ISO/IEC 27003:2010, ISO/IEC 27004:2009, ISO/IEC 27005:2011</p> <p><b>Teaching and Learning Methods:</b> See Assessment</p>
--

### Part 3: Assessment

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.

First Sit Components	Final Assessment	Element weighting	Description
Report - Component B		50 %	Written assignment / report (2000 words) on a selected case study
Examination - Component A	✓	50 %	Written examination (2 hours)
Resit Components	Final Assessment	Element weighting	Description

STUDENT AND ACADEMIC SERVICES

Report - Component B		50 %	Written assignment / report (2000 words) on a selected case study
Examination - Component A	✓	50 %	Written examination (2 hours)

<b>Part 4: Teaching and Learning Methods</b>																			
Learning Outcomes	<p>On successful completion of this module students will be able to:</p> <table border="1"> <thead> <tr> <th colspan="2" style="text-align: center;"><b>Module Learning Outcomes</b></th> </tr> </thead> <tbody> <tr> <td>MO1</td> <td>Demonstrate a deep and systematic understanding of conventional and contemporary ICS implementations and their comparison to IT systems in the context of cyber security</td> </tr> <tr> <td>MO2</td> <td>Undertake the analysis of the cyber threat landscape in ICS and evaluate current cyber protection approaches in the field</td> </tr> <tr> <td>MO3</td> <td>Design and evaluate improvements in current cyber protection approaches to tackle the cyber security challenges that arise in ICS</td> </tr> <tr> <td>MO4</td> <td>Select appropriate risk modelling methods in ICS and critically evaluate their effectiveness on risk measurement</td> </tr> <tr> <td>MO5</td> <td>Critically apply the Kill Chain process to model complex cyber security incident scenarios in ICS and develop situational awareness</td> </tr> <tr> <td>MO6</td> <td>Demonstrate an understanding of industry-specific regulations and standards for the protection of ICS</td> </tr> </tbody> </table>	<b>Module Learning Outcomes</b>		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	MO2	Undertake the analysis of the cyber threat landscape in ICS and evaluate current cyber protection approaches in the field	MO3	Design and evaluate improvements in current cyber protection approaches to tackle the cyber security challenges that arise in ICS	MO4	Select appropriate risk modelling methods in ICS and critically evaluate their effectiveness on risk measurement	MO5	Critically apply the Kill Chain process to model complex cyber security incident scenarios in ICS and develop situational awareness	MO6	Demonstrate an understanding of industry-specific regulations and standards for the protection of ICS				
<b>Module Learning Outcomes</b>																			
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																		
MO2	Undertake the analysis of the cyber threat landscape in ICS and evaluate current cyber protection approaches in the field																		
MO3	Design and evaluate improvements in current cyber protection approaches to tackle the cyber security challenges that arise in ICS																		
MO4	Select appropriate risk modelling methods in ICS and critically evaluate their effectiveness on risk measurement																		
MO5	Critically apply the Kill Chain process to model complex cyber security incident scenarios in ICS and develop situational awareness																		
MO6	Demonstrate an understanding of industry-specific regulations and standards for the protection of ICS																		
Contact Hours	<table border="1"> <thead> <tr> <th colspan="2" style="text-align: center;"><b>Contact Hours</b></th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"><b>Independent Study Hours:</b></td> </tr> <tr> <td style="text-align: center;">Independent study/self-guided study</td> <td style="text-align: center;">114</td> </tr> <tr> <td style="text-align: center;"><b>Total Independent Study Hours:</b></td> <td style="text-align: center;">114</td> </tr> <tr> <td colspan="2" style="text-align: center;"><b>Scheduled Learning and Teaching Hours:</b></td> </tr> <tr> <td style="text-align: center;">Face-to-face learning</td> <td style="text-align: center;">36</td> </tr> <tr> <td style="text-align: center;"><b>Total Scheduled Learning and Teaching Hours:</b></td> <td style="text-align: center;">36</td> </tr> <tr> <td style="text-align: center;"><b>Hours to be allocated</b></td> <td style="text-align: center;">150</td> </tr> <tr> <td style="text-align: center;"><b>Allocated Hours</b></td> <td style="text-align: center;">150</td> </tr> </tbody> </table>	<b>Contact Hours</b>		<b>Independent Study Hours:</b>		Independent study/self-guided study	114	<b>Total Independent Study Hours:</b>	114	<b>Scheduled Learning and Teaching Hours:</b>		Face-to-face learning	36	<b>Total Scheduled Learning and Teaching Hours:</b>	36	<b>Hours to be allocated</b>	150	<b>Allocated Hours</b>	150
<b>Contact Hours</b>																			
<b>Independent Study Hours:</b>																			
Independent study/self-guided study	114																		
<b>Total Independent Study Hours:</b>	114																		
<b>Scheduled Learning and Teaching Hours:</b>																			
Face-to-face learning	36																		
<b>Total Scheduled Learning and Teaching Hours:</b>	36																		
<b>Hours to be allocated</b>	150																		
<b>Allocated Hours</b>	150																		
Reading List	<p><i>The reading list for this module can be accessed via the following link:</i></p> <p><a href="https://uwe.rl.talis.com/modules/ufcf7p-15-m.html">https://uwe.rl.talis.com/modules/ufcf7p-15-m.html</a></p>																		