Coursework Sepcification

Module details

Module Code	**UFCF7P-15-M**
Module Title	**Critical Systems Security (CSS)**
Module Leader	**Jonathon Stadon**
Module Tutors	**Phil Legg, Ian, thomas, Gwyn, Jonathan White**
Year	**2020-21**
Component/Element number	**CompB/E1**
Total number of assessments for this module	**2**
Weighting	**50%**
Element description	**2000 – 3000 Written report**

Dates

Submission Date	**5 August 2021**
Submission place	**Blackbaord, Assignments**
Submission time	**14:00 (2pm)**
Submission notes	**Please ensure that you work is submitted in an accessable format. (Ideally a Docx or PDF)**

Feedback

Feedback provision will be	**Feedback will be published through Blackbaord. If you would like additional feedback, then please contacts your leader/tutor to arrange a meeting.**

Contents

Section 1: Overview of Assessment

This assignment assesses the following module learning outcomes:

- Demonstrate a deep and systematic understanding of conventional and contemporary ICS implementations and their comparison to IT systems in the context of cyber security; (A, B)
- Undertake the analysis of the cyber threat landscape in ICS and evaluate current cyber protection approaches in the field; (B)
- Design and evaluate improvements in current cyber protection approaches to tackle the cyber security challenges that arise in ICS. (B)

The assignment is worth ***50%*** of the overall mark for the module.

Broadly speaking, the assignment requires you to write a 2,000-3,000 word report on the analysis of the current cyber threat landscape and cyber protection approaches in the Critical Infrastructure, proposing ways for improvement. The report will be research-based, written in an industrial standards format; you are expected to draw information from one or more case studies including but not limited to “Stuxnet” (and/or variations of Stuxnet), the “Analysis of the Cyber Attack on the Ukrainian Power Grid” in 2015 and Wannacry.

The assignment is described in more detail in section 2.

This is an individual assignment.

Working on this assignment will help you to identify and analyse the challenges that arise in the cyber protection of cyber physical control systems used in the Critical Infrastructure, and present them in a report that follows industrial standards. Through your research you will analyse and evaluate the current threat landscape and the cyber protection approaches in the field, and propose ways for improvement. If you have questions about this assignment, please post them to the discussion board on Blackboard.

Section 2: Task Specification

Produce a 2,000 words report analysing selected case study/-ies on cyber security incidents in the Critical Infrastructure.

You are working as an independent consultant for a Cyber Security firm that operates a Research and Development department on Cyber Security in Industrial Control Systems. The firm wants to gather intelligence on cyber security in Critical Systems in order to come up with new products and solutions. Your assignment is to do research in this area and produce a report that addresses the firm's needs. In particular, your research will focus on:

- The analysis of the current threat landscape in cyber physical control systems used in the Critical Infrastructure.
- The analysis and evaluation of current cyber-security approaches in the field.
- Ways to improve current cyber security approaches, analysing their impact on the system.

Your research must draw information from one or more case studies provided in the lectures (e.g. Stuxnet, Flame, Ukrainian Power Grid, Wannacry etc.) and relevant papers of high quality. In your report, you must clearly identify the following elements:

- The differences between traditional IT systems and Critical Systems and how they affect cyber security;
- The entities involved in cyber security incidents in the Critical Infrastructure (e.g. attack actors, ICS vendors, environment etc.);
- The cyber security risks and the associated threat vectors;
- Current cyber security approaches and their limitations, analysing the technical and operational challenges that arise;
- Ways to improve cyber security in this area, discussing their impact on the system.

The report must follow professional standards, written in an appropriate style and format. Accuracy, completeness and consistency of citation and listing of sources must also be taken into account.

Section 3: Deliverables

A 2,000-3,000 word written report is to be submitted via Blackboard by XXX in PDF format.

Your report should include the result of your research as described in Section 2. On the first page of your report you should clearly identify the subject/title of the report, your name and surname followed by your student ID and the current date.

Section 4: Marking Criteria

	0-29	30-39	40-49	50-59	60-69	70-84	85-100	Mark & Advice for Improvement
Understanding the nature of ICS (differences with IT systems and impact on cyber security in ICS) (25%)	Poor content; little or no description of the differences between IT and ICS systems.	Provides some description of the differences between IT systems and ICS; content not adequate; further analysis is needed on the impact they have on cyber security.	Provides a description of the differences between IT systems and ICS; impact analysis could be clearer.	Provides a well written description of the differences between IT systems and ICS, giving an impact analysis based on information drawn from good quality sources.	Very well written description of the differences between IT systems and ICS based on high quality sources; provides a well written impact analysis based on high quality sources.	Excellent description of the differences between IT and ICS systems, explaining in detail how they affect cyber security in ICS. Appropriate sources used.	Outstanding description of the differences between IT and ICS systems and how they affect cyber security, providing examples from case studies; use of additional sources.; publishable material.	
Analysis of the threat landscape and evaluation of current cyber-	Poor content; little or no analysis of the threat landscape and/or evaluation of current cyber	Provides some analysis of current threat landscape and security approaches; misses	Provides a description of the landscape and some evaluation of current cyber	Provides a well written description of the threat landscape and an evaluation of	Provides a very well written description of the threat landscape and an	Excellent analysis of the threat landscape and current cyber security	Outstanding analysis of the threat landscape and current cyber security	

security approaches (25%)	security approaches.	important elements; inadequate depth of content.	security approaches.	current cyber security approaches based on data drawn from good quality sources.	evaluation of current cyber security approaches based on data drawn from high quality sources.	approaches; appropriate sources used.	approaches, providing examples from case studies; use of additional sources; publishable material.	
Ways to improve current cyber security approaches (25%)	Poor content; little or no discussion on ways to improve cyber security in ICS.	Some suggestions on how to improve cyber security in ICS; inadequate content; little or no evaluation of the proposed methods.	Provides suggestions to improve cyber security in ICS; not clear how they map to the rest of the report; provides some evaluation of proposed improvements.	Well written suggestions on how to improve cyber security in ICS; based on the analysis of current approaches; provides evaluation of proposed improvements.	Very well written suggestions on how to improve cyber security in ICS; based on detailed analysis of current approaches; provides evaluation of proposed improvements.	Excellent work on suggestions to improve cyber security in ICS; based on detailed analysis of current approaches as identified in relevant papers or case studies; well-presented evaluation of proposed improvements.	Outstanding work on suggestions to improve cyber security in ICS; based on detailed analysis of current approaches as identified in relevant papers and case studies. Publishable material; well-presented evaluation of proposed improvements.	

Quality of writing (25%)	No use of the appropriate terminology; fails to describe the problem and the work done; shows a lack of structure, comprehensibility, clarity and grammatical quality.	Lack of or inaccurate use of the appropriate terminology; shows a lack of structure, comprehensibility, clarity and grammatical quality.	Often fails to use appropriate terminology; may lack in layout and/or logical structure; may show a lack of clarity and comprehensibility; lacking grammatical structure.	Mostly uses appropriate terminology; well presented; lacking in clarity and grammatical structure.	A good grasp of the appropriate terminology; well presented in both layout on the page and logical structure; resented in an appropriate style; good grammatical standard.	Uses appropriate terminology accurately; professionally presented in both layout on the page and logical structure; very well presented in an appropriate style; grammatically of a very high standard.	Uses appropriate terminology accurately; professionally presented in both layout on the page and logical structure; impressively presented in an appropriate style; grammatically of an extremely high standard.	