

The Villanova University
Master of Science in Cybersecurity
Department of Electrical and Computer Engineering
ECE 8485 Industrial Control Systems Security
August 17 – December 5, Fall 2020

Instructor:

Dr. Charles Pak

Email: charles.pak@villanova.edu; charlespak1@outlook.com

Email is the best way to contact me. Here is my cell number if needed: (410)805-2110

Live Session Zoom Account: <https://villanova.zoom.us/j/4041504589>

General Course Information:

This is a graduate level class. Students are expected to apply time management skills to their work, home, and academic life. Any due dates for materials for these classes are designed to spread the workload over the semester. Material, such as reading assignments, with no due date given should be done as soon as possible by the student so the workload does not become overwhelming prior to the end of course.

Course Description

Students will address basic security concepts as they apply to critical infrastructure systems. Concepts addressed in the course will include Industrial Control Systems (ICS), such as Supervisory and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), national standards for the protection of critical infrastructure, and risk management concepts and tools for critical infrastructure systems. Students will perform a risk assessment of a specific critical infrastructure sector using an appropriate risk assessment framework and tools, identifying threats and vulnerabilities specific to the sector, and making appropriate recommendations for mitigating risk.

Course Objectives

Upon completion of this course, the student will be able to:

- Define CI sectors and identify legislation and standards addressing CI protection.
- Define common terms and concepts associated with CI, including ICS, SCADA, PCS, and DCS.
- Identify the components and process of implementing a CISR (Critical Infrastructure Security and Resilience) risk management program.
- Describe cybersecurity services such as confidentiality, integrity, availability, and authentication as they apply to critical infrastructure systems.
- Select appropriate vulnerability assessment frameworks and tools as a part of a risk assessment of a CI system.
- Identify and describe cybersecurity threats, risks, vulnerabilities, and attacks as they apply to CI systems.
- Identify an appropriate risk management strategy for CISR.

Required Reading Materials:

There is no official textbook for this course.

A Cybati Vimeo course (over 10 hours of content) will be made available to students. PDF files related to this material will also be made available. Students are expected to review the modules of this vimeo course on a timed schedule as indicated in the course schedule. In addition, the class will feature numerous resources that will be posted on Blackboard. Included is an extensive set of modules on Critical Infrastructure Security developed under NSF funding by CyberWatch West.

Villanova is in the process of creating a CyberPhysical Systems Security Lab (CEER 307) and will be acquiring

instructional materials from Cybati and other vendors to support the lab. Some of them may be used during the summer session.

Policy on Paper Submission

Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. Please note that life emergencies happen. Do NOT wait until the last moment to start on your paper. If you do that and something comes up to impede your progress, it will hamper your ability to turn in your paper on time. Papers MUST be submitted electronically via Blackboard.

All papers must include the following statement:

“This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word ‘Signature’, I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____”

Reading Assignments:

The scope of this course is very broad, and a large amount of reading is required. However, the relative importance of materials, as specified in the course outline, varies. Specifically assigned materials must be read in detail. Materials to which students are directed or for which copies are provided but which are not specifically assigned are recommended for added understanding of required material, but are optional in the sense that students will not be held explicitly responsible for anything that appears only in these materials. They are appropriate either for students who have difficulty with the subject matter based on the required readings or for those who want a deeper understanding of the material. Recommended background reading is valuable for overall understanding, may provide a technical depth beyond the requirements of the class, may provide valuable material for student research topics, and may be useful in responding to comprehensive essay questions.

Since much of what is happening in information security is happening now, current events will play a role in class discussions. As professionals, it is crucial for you to keep up with events as they unfold. There is no substitute for regular reading of business and technology news in a major newspaper, for following current journal articles, visiting key web sites, and for noting the direction of industry organizations such as the IEEE, IETF, and the ACM. You should constantly consider how what you read in such sources fits into the subject you are studying. Current articles, including Web articles, may be assigned as supplementary reading as the course progresses.

Students are encouraged to use as many and varied sources as possible in exploring the questions presented during the course, and to share those sources with their classmates. References to sources should be explicit in exchanges among the students and instructor, and will be considered in determining the extent to which each student participated for purposes of awarding grades.

Research Papers:

The student will prepare three research papers on the Power Grid Security Control Systems, Water Control Systems, Gas, Oil, and Chemical Industrial Systems vulnerabilities with recommended security controls. Details must be included in each paper to describe the critical systems operational procedures, associated vulnerabilities, cyberattacks, breaches with supporting examples of evidence. Each critical infrastructure system may have inherent vulnerabilities, and experienced cyber attacks due to these known vulnerabilities.

Presentation Slide Deck:

The student will prepare for the presentation slide deck to present his/her research findings of three research paper topics and share the presentation slide deck with the class. During the final week, the student will submit his/her recorded presentation slide deck.

Grading Policy:

The overall course grade will be established as follows:

Grading Criteria	Percentage
Discussion Participation	15
Power Grid Security Control System Research Paper	25
Water Control System Research Paper	25
Gas, Oil, and Chemical Industrial Systems Research Paper	25
Recorded Research Presentation Slide Deck	10
Total	100

http://www1.villanova.edu/villanova/enroll/registrar/policies.html#question_faq_5

Letter Grade Approximate percentage grade range Grade Points

A	95–100	4.00
A–	90 < 95	3.67
B+	85 < 90	3.33
B	80 < 85	3.00
B–	75 < 80	2.67
C+	70 < 75	2.33
C	65 < 70	2.00
F	< 65	0.00

Other Items of Importance

Don't ask for an incomplete for convenience. The University has very specific policy on when a grade of incomplete may be awarded. See the Bulletin for more information on grading policies.

Writing and Speaking Standards:

Written communication is an important element of the total communication process. This is a graduate program. **Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.** The University recognizes and expects exemplary writing to be the norm for course work. To this end, all papers, individual and group, must demonstrate graduate level writing and comply with and conform to standard academic format as specified in A Manual For Writers of Term Papers, Theses, and Dissertations by Kate L. Turabian, Seventh Edition. Points will be subtracted for format errors. Points will also be subtracted for spelling and grammatical errors. Use of Standard English ensures that your points will be both understood and correctly interpreted by all readers, a skill that will be vital to your success after graduation.

Effective managers, leaders, and teachers are also effective communicators. It is no understatement to say that effective speaking and writing skills are as important to career success as technical mastery of a subject. Speaking and writing effectively are a critical part of this course. Correct and graduate level Standard English must be used.

Academic integrity:

Academic integrity is central to the learning and teaching process. Students are expected to conduct themselves in a manner that will contribute to the maintenance of academic integrity by making all reasonable efforts to prevent the occurrence of academic dishonesty. Academic dishonesty includes, but is not limited to, obtaining or giving aid on

an examination, having unauthorized prior knowledge of an examination, doing work for another student, and plagiarism of all types.

Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to, the following: copying verbatim all or part of another's written work; using phrases, charts, figures, illustrations, or mathematical or scientific solutions without citing the source; paraphrasing ideas, conclusions, or research without citing the source; and using all or part of a literary plot, poem, film, musical score, or other artistic product without attributing the work to its creator. Students can avoid unintentional plagiarism by following carefully accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources.

There is no such thing as “boilerplate” in academia.

If you don't understand what plagiarism is and how to avoid it, consult the University's academic integrity policy.

See also http://www.prism-magazine.org/december/html/student_plagiarism_in_an_onlin.htm

This is a graduate program. Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.

The penalties for plagiarism include a zero or a grade of “F” on the work in question, a grade of “F” in the course, suspension with a file letter, suspension with a transcript notation, or expulsion. Students are not permitted to submit an assignment or paper that already has been submitted for another course at any institution, even if it is entirely their own work. This includes cutting and pasting portions of previous papers or other written assignments. The penalties will be the same as those listed above for plagiarism. Please check your work carefully. Turabian contains complete guidance on how to correctly reference all forms of material.

There is no such thing as “boilerplate” or “standard language” in academia. Students are expected to write their reports themselves. If it is necessary to use material from other sources, it is expected (and mandatory) that the standards of academic style and integrity will be followed. Every student is encouraged to visit these websites for interesting information regarding this issue:

- A true story about plagiarism gone awry

http://www.aweekofkindness.com/blog/archives/the_laura_k_krishna_saga/000023.html (May only be available in a Google Cache as Domain expired 2/23/2011).

- Goucher College's “Plagiarism-by-Paraphrase Risk Quiz”

<http://faculty.goucher.edu/writingprogram/sgarrett/Default.html>

- Copyright law, frequently asked questions, and other good stuff

<http://www.copyright.gov/>

- The Islam Online.net Fatwa on Plagiarism

http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503549102

Disabled Students: Any student who has a disability and is in need of special consideration must inform the instructor of this need within the first week of class (or immediately if the disability appears after the first week of class) so that appropriate arrangements can be made. This includes students with reading or learning disabilities who may require extra time on tests. In all cases, the student must communicate with the Disability Services Center and have registered the disability with the University.

Discussion Rubric

Criteria	Non-compliant	Minimal	Compliant	Advanced
One initial major response (minimum 125 words) to first discussion question	Did not complete this portion of the assignment or most of the discussion points were inappropriate or were not identified. (1)	The discussion points were identified and described but with fair accuracy and some of the discussion points were inappropriate or were not identified. (3)	The discussion points were identified and described with good accuracy and appropriate information was identified and discussed. (6)	The discussion points were identified and described with high accuracy and all appropriate information was identified and discussed clearly. (10)
Writing – grammar, sentence structure, paragraph structure, spelling, punctuation (APA required).	5 or more different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References are expected. (Major issues) (1)	3-4 different errors in sentence structure, paragraph structure, or APA usage. References are expected. (Many issues) (3)	1-2 different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References are expected. (Minor issues) (6)	No errors in sentence structure, paragraph structure, spelling, punctuation or APA usage. References are expected. (Minor issues) (10)
Responding to other students.	Did not respond to other students or responses were trite with no substance. (1)	Responded to other students but responses were trite with no substance. (3)	Responded to one other student, response was substantive. (6)	Responded to two or more other students, responses were substantive. (10)
Frequency of responses.	Did not post in the threaded discussion. (1)	Posted one message only 1 day of the week. (3)	Posted more than 1 message but only one day of the week. (6)	Posted on two or more different days of the week. (10)

Course Schedule (Tentative as of 8/15/20)

Wk	Date	Discussion Topic	Assignments
1	8/17	Module 1 Cybati Vimeo Sections 1.0 through 1.4; CI Module 1: CI Introduction, CI Module 2: Intro to Control Systems and SCADA; Lab 1 Cybati VM Setup; Yellowdig Think	Discussion Participation
2	8/24	Continue Module 1 Cybati Vimeo Sections 1.0 through 1.4; CI Module 1: CI Introduction, CI Module 2: Intro to Control Systems and SCADA; Lab 1 Cybati VM Setup; Yellowdig Think	Discussion Participation
3	8/31	Module 2 Cybati Vimeo Sections 1.5 through 1.8; CI Module 3: Technologies; VoiceThread Get Acquainted; Lab 2 Virtual Bottling Plant; TGS #2; Lab Equipment acquisition complete	Discussion Participation
4	9/7	Continue Module 2 Cybati Vimeo Sections 1.5 through 1.8; CI Module 3: Technologies; VoiceThread Get Acquainted;	Discussion Participation

		Lab 2 Virtual Bottling Plant; TGS #2; Lab Equipment acquisition complete	
5	9/14	Module 3 Cybati Vimeo Sections 2.0 through 2.3; CI Module 4: Risk Management; TGS #3; Lab 3 Lab Equipment Operational	Discussion Participation
6	9/21	Continue Module 3 Cybati Vimeo Sections 2.0 through 2.3; CI Module 4: Risk Management; TGS #3; Lab 3 Lab Equipment Operational	Power Grid Security Control System Research Paper Discussion Participation
7	9/28	Module 4 Cybati Vimeo Sections 2.4 through 2.8; CI Module 5: Threats, CI Module 6: Vulnerabilities; Lab 4 Raspberry Pi Traffic Light Part 1; TGS #4	Online Commerce Protection Paper Discussion Participation
8	10/5	Continue Module 4 Cybati Vimeo Sections 2.4 through 2.8; CI Module 5: Threats, CI Module 6: Vulnerabilities; Lab 4 Raspberry Pi Traffic Light Part 1; TGS #4	Discussion Participation Presentation Slide Deck
9	10/12	Module 5 Cybati Vimeo Section 3; CI Module 8 Remediation; Lab 5 Raspberry Pi Traffic Light Part 2; TGS #5	Water Control System Security Research Paper Discussion Participation
10	10/19	Continue Module 5 Cybati Vimeo Section 3; CI Module 8 Remediation; Lab 5 Raspberry Pi Traffic Light Part 2; TGS #5	Discussion Participation
11	10/26	Module 6 Cybati Vimeo Section 4; CI Module 9 Incident Response; VoiceThread Submission due; TGS #6	Discussion Participation
12	11/2	Continue Module 6 Cybati Vimeo Section 4; CI Module 9 Incident Response; VoiceThread Submission due; TGS #6	Discussion Participation
13	11/9	Module 7 Cybati Vimeo Section 4; CI Module 9 Incident Response; VoiceThread Submission due; TGS #6	Discussion Participation
14	11/16	Continue Module 7 Cybati Vimeo Section 4; CI Module 9 Incident Response; VoiceThread Submission due; TGS #6	Gas, Oil, and Chemical Industrial Systems Security Research Paper Discussion Participation
15	11/23	Module 8 – Thanksgiving Holiday Week - No Live Session	

		CI Module 11 Trends; Semester Review; Final Exam due in 1 Week	Discussion Participation
16	11/30	Final Week Submit a Recorded Research Paper Presentation, inclusive of all three research papers	Recorded Research Papers Presentation

Research Paper Grading Rubric

Criteria					
	Poor	Fair	Good	Excellent	Percent
Organization	Sequence of information is difficult to follow. (0 – 7)	Reader has difficulty following work because student jumps around. (8 – 14)	Student presents information in logical sequence which reader can follow. (15 – 22)	Information in logical, interesting sequence which reader can follow. (23 – 30)	30%
Content Knowledge	Student does not have grasp of information; student cannot answer questions about subject. (0 – 12)	Student is uncomfortable with content and is able to demonstrate basic concepts. (13 – 24)	Student is at ease with content, but fails to elaborate. (25 – 37)	Student demonstrates full knowledge (more than required). (38 – 50)	50%
Grammar and Spelling	Work has significant spelling errors and/or grammatical errors. (0 – 2)	Presentation has several and/or grammatical errors. (3 – 4)	Presentation has a couple misspellings and/or grammatical errors. (5 – 7)	Presentation has no misspellings or grammatical errors. (8 – 10)	10%
APA Formatting	Work has significant formatting errors (i.e. references page, title page, spacing, citations). (0 – 2)	Work has several formatting errors (i.e. references page, title page, spacing, citations). (3 – 4)	Work has a few formatting errors (i.e. references page, title page, spacing, citations). (5 – 7)	Work has no formatting errors (i.e. references page, title page, spacing, citations). (8 – 10)	10%