CSCI 497.1SW, Industrial Control System (ICS) Cyber Security

COURSE SYLLABUS: Fall 2021

INSTRUCTOR INFORMATION

Instructor:	Joel Langill
Office Location:	Virtual via Zoom/PHone
Office Hours:	By appointment
Office Phone:	(920) 594-0321
Office Fax:	n/a
University Email Address:	joel.langill@tamuc.edu
Preferred Form of Communication:	Moodle LMS Message / Email
Communication Response Time:	Within 24 hours on weekdays. If emails are sent on Friday, response will be available by the following Monday.

COURSE INFORMATION

Weekly Lecture: Mo 5:00 – 7:30 pm - Virtual Classroom via Zoom
Labs, Case Studies and Demonstrations will take place during select Weekly Lecture periods.

Materials – Textbooks, Readings, Supplementary Readings

Textbook Required:	*"Industrial Network Security"*, 2nd edition by Knapp and Langill, Elsevier/Syngress, ISBN 978-0-12-420114-9
Software Required:	Wireshark (free) NetworkMiner (free) Grass Marlin (free) (websites and instructions provided in lab)

The *syllabus/schedule are subject to change.*

Software Optional: Ubuntu Linux 18.04LTS or later (or any current distro)
Kali Linux 2020 or later
VMware Workstation Pro 14 or later (Windows/Linux)
or
VMware Fusion 10 or later (Mac)
or
Oracle VirtualBox 5.2 or later (Windows/Mac/Linux)
or
Microsoft Hyper-V (Windows 8/Server 2012)

Textbooks Optional: *"Hacking Exposed: Industrial Control Systems"*,
by Bodungen, Singer, et al,
McGraw Hill, ISBN 978-1-25-958971-3

"Applied Cyber Security and the Smart Grid",
by Knapp and Samani,
Elsevier/Syngress, ISBN 978-1-59749-998-9

Course Description

This is a lecture and laboratory course designed to introduce concepts around cyber security of industrial (ICS) and facility-related control systems (FRCS). The course presents ICS/FRCS in terms of their operation, design, and architecture. Foundational principles of cyber security as it applies to ICS/FRCS are introduced through a combination of lectures, lab exercises, and demonstrations using real-world equipment. A risk management framework is discussed, and how this applies to assessing the security posture of operational technologies in terms of identification of assets, characterization of their communication methods, and discovery of vulnerabilities that cover both inherent asset weaknesses and those introduced through system design and operation.

Student Learning Outcomes

Most of the concepts introduced in this course will be applied as part of lab exercises and homework assignments. At the end of the course, students will be able to:

1. Understand ICS architectures, their components, and their operation
2. Explain the differences between information and operational technologies
3. Identify unique threats and vulnerabilities within ICS architectures
4. Collect network traffic and analyze protocols
5. Inventory ICS hardware and software
6. Characterize communication flows within an ICS architecture
7. Identify and mitigate vulnerabilities within an ICS architecture
8. Perform cyber security audits and baselines against networked assets
9. Apply the components of risk management to cyber security
10. Learn about leading industry standards and best practices for industrial security

The *syllabus/schedule are subject to change.*

COURSE REQUIREMENTS

Minimal Technical Skills Needed

Students enrolling in this course should have mastered basic computer skills including both graphical and command line interfaces. Students should be proficient with typical office productivity software (Microsoft Word, Excel, PowerPoint, and Visio), text editors, and Web browsers. A small number of labs are performed on student owned computers, so they should be authorized and able to download, install, and configure software. It is helpful for students to be comfortable working in both Microsoft Windows and Linux operating systems and possess basic networking knowledge. Additional material is provided to assist students in any areas that require individual development and improvement if they do not possess prior knowledge. Students will be introduced to virtualization technologies to build and use systems outside of the classroom. This course will be integrated with the Moodle LMS to manage assignments, lecture material, lab exercises, and reference information.

Instructional Methods

This course utilizes four (4) complimentary components to introduce, reinforce and apply the material covered. Standard presentation-based lectures delivered via a virtual classroom (Cisco Webex, Microsoft Teams, Google Meet, Zoom, etc.) comprise approximately 50% of the allotted time. Students will engage in a variety of hands-on exercises to expand on lecture material, including a practical assessment of an ICS designed to replicate an actual field cyber security exercise. These exercises compromise approximately 40% of the course time. The remaining 10% consists of instructor-led demonstrations of relevant industrial security technologies. If time allows, students may also be given the opportunity to participate in case studies that provide an opportunity to review, analyze and learn from actual ICS cyber events.

Tips for Success in the Course

1. Plan to spend approximately three (3) hours of work outside of class each week for reading assignments, exercises, and personal review of reference material.
2. Attend all lectures and lab sessions to interact with the instructor and classmates.
3. Read textbook before lecture.
4. Review supplemental material on the Moodle LMS following each lecture and read articles that address your interest or areas needing additional attention. Consider this site your personal tutor.
5. If you do not understand something, ask a question. An effort will be made to have time for questions at the end of each lecture.
6. Consider creating your own home lab using virtualization techniques and readily available free software.
7. Use your home lab to experiment with the tools that are introduced in class. The more you practice, the more you will learn and the better your skills will become.

The *syllabus/schedule are subject to change.*

GRADING

Letter grades for this course will be based on the following scale:

A	90% - 100%
B	80% - 89%
C	70% - 79%
D	60% - 69%
F	59% or Below

All grades will be determined from a straight scale with no curve. Some course components will be graded on a “pass” or “fail” basis. A “pass” grade will be given for completion of all the requirements of the component. For example, a “pass” grade will be given for a student that completes and submits in a timely manner all lab exercises. The final grade calculation may be based on “curve” at instructor’s discretion and will be applied equally to all students.

Assessments

Course numeric scores calculated at the end-of-semester will be weighted as follows:

Component	**Percentage**	**Grade Method**
Quizzes	20%	Graded Score
Assignments	20%	Pass / Fail
Lab Exercises	20%	Pass / Fail
Term Paper	20%	Graded Score
Final Examination	20%	Graded Score

This course will only be delivered in a virtual classroom setting. Students should do their own work on assignments, labs, quizzes, and exams. Copying another student’s work is not acceptable. Any indication of cheating or plagiarism on any course component will result in an automatic 0 (zero) for the activity for all students involved. Continued violation of this policy will be subject to published academic policies up to including a failing grade for the course. Please refer to “Academic Honesty” under “Course Specific Procedures/Policies” in this syllabus for additional details.

Quizzes

Quizzes are graded based on the correctness of the answers. Quizzes are administered after each of the major lecture modules of this course and are distributed over the semester. They are focused on the material covered in the module and are not considered comprehensive for all prior material covered to date. Quizzes will be made available on the Moodle LMS following the delivery of the lecture and must be completed by 8:00am the day before the next scheduled class session. Quizzes will be timed and will allow questions to be skipped and answered later in the quiz. Grades will

be available in both the Moodle LMS and D2L. There will be no make-ups for any missed quiz due to the virtual classroom environment and the flexibility to connect to the LMS and take the quiz any time during the test period. Students should contact the instructor in the case of extenuating circumstances (e.g. illness, accident, etc.). These situations will be reviewed as needed on a case-by-case basis.

Assignments/Lab Exercises

Assignments and/or lab exercises will be distributed weekly. Assignments should be completed outside of the normal lecture session. Time is allocated for labs to be completed during the weekly scheduled time for the class and will be done in lieu of a formal lecture with the instructor available for questions. Assignments and lab exercises should be completed independently. Cyber security is a field that involves working in teams, so some collaboration with other classmates is acceptable and encouraged. All assignments and lab exercises must be completed and uploaded into the Moodle LMS by 8:00am the day before the next class session. Email shall not be used to submit assignments and lab exercises. Grades will be available in both the Moodle LMS and D2L. Late assignments or lab exercises will not be allowed due to the virtual classroom environment and the flexibility to connect to the LMS and conduct the lab or submit the assignment any time during the period. Students should contact the instructor in the case of extenuating circumstances (e.g. illness, accident, etc.). These situations will be reviewed as needed on a case-by-case basis.

Term Paper

Each student will be required to write a six (6) to ten (10) page term paper during the semester. Topic selection and specific requirements will be provided at mid-term and are due at course time scheduled for Week 14. Each student will pick from a provided list of common industrial control systems and will develop in the paper the following topics:

1. System architecture covering devices and network topology
2. Industry sectors that typically use the system
3. Communication protocols used by the system
4. Vulnerabilities publicly discovered for the system
5. Cyber security measures taken by the vendor to secure the system
6. Impact of the vulnerabilities discovered to the industry sectors served

Each student will present a brief presentation during the final session in Week 15. Papers will be written using either APA or MLA style guide. Grading will be based on the following:

Ideas and Analysis	20%
Organization	20%
Development and Support	20%
Style	10%

The *syllabus/schedule are subject to change.*

Mechanics	20%
Presentation	10%

Students are given six (6) weeks to complete this paper and are encouraged to use this time to develop a clear, description, and concise paper. A course outline will be required two (2) weeks prior to the submission deadline.

Final Examination

A final examination will be administered during the regular scheduled time during Week 16 and will be posted on the Moodle LMS. All students MUST take the exam at the same time. Students should contact the instructor if there are any conflicts with the test time allowing an alternate to be arranged. This exam will be administered through the Moodle LMS. The exam is graded based on the correctness of the answers. The exam will be timed and will allow questions to be skipped and answered later in the exam. Grades will be available in both the Moodle LMS and D2L within one (1) day of the exam. Students should contact the instructor in the case of extenuating circumstances (e.g., illness, accident, etc.). These situations will be reviewed as needed on a case-by-case basis.

Bonus / Extra Credit and Borderline Grades

Students may be awarded bonus credit is certain cases according to the quality, completion, and or creativity of assignments, labs, term paper, quizzes, and exams. Borderline grades may be affected positively or negatively by class participation, attendance, attitude, and class etiquette (e.g., no sound-producing devices, avoid distracting other students, etc.).

TECHNOLOGY REQUIREMENTS

Learning Management System (LMS)

All course sections offered by Texas A&M University-Commerce have a corresponding course shell in the myLeo Online Learning Management System (LMS). Below are technical requirements

LMS Requirements:
https://community.brightspace.com/s/article/Brightspace-Platform-Requirements

LMS Browser Support:
https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

YouSeeU Virtual Classroom Requirements:
https://support.youseeu.com/hc/en-us/articles/115007031107-Basic-System-Requirements

The *syllabus/schedule are subject to change.*

Lab LMS

This course is augmented with a specialized LMS based on the Moodle learning platform. This infrastructure provides HTML5 access using a standard Web browser to sandboxed systems utilized in the labs, as well as providing an expansive repository of reference information to supplement the lecture material. Recordings of all lectures will also be placed on the Moodle LMS. Cookies must be enabled to use the Moodle LMS.

Maintenance may be required on the Moodle LMS throughout the semester. All attempts will be to provide maintenance activities on Friday evenings, unless circumstances require immediate attention. Logins will be disabled during maintenance activities.

Moodle LMS Browser Support:
https://docs.moodle.org/dev/Moodle_3.11_release_notes#Browser_support

Access and Navigation

You will need your campus-wide ID (CWID), myLeo credentials, and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu**.**

Note: Personal computer and internet connection problems do not excuse the requirement to complete all course work in a timely and satisfactory manner. Each student needs to have a backup method to deal with these inevitable problems. These methods might include the availability of a backup PC at home or work, the temporary use of a computer at a friend's home, the local library, office service companies, Starbucks, a TAMUC campus open computer lab, etc. All course content is available via standard web browsers and can be accessed via any Internet-connection.

COMMUNICATION AND SUPPORT

Student Support

If you have any questions or are having difficulties with the course material, please contact your Instructor.

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here:
https://community.brightspace.com/support/s/contactsupport

Interaction with Instructor Statement

The instructor will not keep regular scheduled office hours. The instructor will be available immediately after weekly lectures and labs to address general questions and assistance with the course. If students require additional hours, an appointment can be scheduled with the instructor on the Moodle LMS. The recommended method to communicate with the instructor should be using Moodle LMS Messaging (primary) or email (secondary). Requests should be sent to the instructor at least 24 hours prior to the time the student plans on meeting. The instructor will make every effort to reply to messages in a timely manner. A reply can be expected within 24 hours. Telephone calls should be limited to urgent situations.

The instructor's responsibilities shall include:

1. Make sure to accommodate the learning needs of all students
2. Try his best to answer student questions and resolve other related issues
3. Provide feedback and grade assignments within one (1) week of the due date.

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

Quizzes will be taken outside of scheduled course lectures. Quizzes, labs, and assignments must be completed by 8:00am the day before the start of the next class session and are clearly stated for each activity. No late work will be accepted except under special extenuating circumstances. This includes make-up quizzes and examinations due to the virtual classroom structure. All assignments and lab exercises must be submitted using the Moodle LMS. All grades will be posted to D2L within one (1) week after assignment due date. Students are responsible for checking their grades after each activity and must report any error or inconsistency to the instructor within seven (7) days if possible.

Class Decorum: Civility in the classroom or online course and respect for the opinions of other is important in an academic environment. It is likely you may not agree with everything that is said or discussed in the classroom/online course. Courteous behavior and responses are expected. To create and preserve a learning environment that optimizes teaching and learning, all participants share a responsibility in creating a civil and nondisruptive forum. Students are expected to conduct themselves at all times in a manner that does not disrupt teaching or learning. Faculty have the authority to request students who exhibit inappropriate behavior to leave the class/online course and may refer serious offenses to the University Police Department and/or the Dean of Students for disciplinary action. (See Student Guidebook)

Academic Honesty: It is the policy of the University, the College of Science and Engineering, the Computer Science and Information Systems department, and the instructor that no form of plagiarism or cheating will be tolerated. Plagiarism is defined as the deliberate use of another's work and claiming it as one's own. This means ideas

as well as text, whether paraphrased or presented verbatim (word-for-word). Cheating is defined as obtaining unauthorized assistance on any assignment. Collusion is defined as selling or purchasing academic products with the intention that they be submitted to fulfill an academic or course requirement. Proper citation of sources must always be utilized thoroughly and accurately. Cheating. Plagiarism, and/or collusion will result in a grade of "0" on the assignment and may also result in a failing grade of "F" for the course and/or disciplinary action by the University. Any student found guilty of violating academic integrity policy will fail the assignment in question, will automatically fail the course and will be subject to disciplinary action by the university (see Texas A&M University-Commerce Code of Student Conduct 5.b. [1,2,3]). Further information on the department's plagiarism policy can be found on the department webpage. If you are unclear about what constitutes academic dishonesty, ask.

Syllabus Change Policy

The syllabus is a guide. Circumstances and events, such as student progress, may make it necessary for the instructor to modify the syllabus during the semester. Any changes made to the syllabus will be announced in advance.

UNIVERSITY SPECIFIC PROCEDURES

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment. The Code of Student Conduct is described in detail in the Student Guidebook.
http://www.tamuc.edu/Admissions/oneStopShop/undergraduateAdmissions/studentGuidebook.aspx

Students should also consult the Rules of Netiquette for more information regarding how to interact with students in an online forum:
https://www.britannica.com/topic/netiquette

TAMUC Attendance

For more information about the attendance policy please visit the Attendance webpage and Procedure 13.99.99.R0.01.
http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.pdf

Academic Integrity

Students at Texas A&M University-Commerce are expected to maintain high standards of integrity and honesty in all of their scholastic work. For more details and the definition of academic dishonesty see the following procedures:

Undergraduate Academic Dishonesty 13.99.99.R0.03

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf

Graduate Student Academic Dishonesty 13.99.99.R0.10

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/graduate/13.99.99.R0.10GraduateStudentAcademicDishonesty.pdf

Students with Disabilities-- ADA Statement

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services
Texas A&M University-Commerce
Gee Library- Room 162
Phone (903) 886-5150 or (903) 886-5835
Fax (903) 468-8148
Email: studentdisabilityservices@tamuc.edu
Website: Office of Student Disability Resources and Services
http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

Nondiscrimination Notice

Texas A&M University-Commerce will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.

Campus Concealed Carry Statement

Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in Texas A&M University-Commerce buildings only by persons who have been issued and are in possession of a Texas License to Carry a Handgun. Qualified law enforcement officers or those who are otherwise authorized to carry a concealed handgun in the State of Texas are also permitted to do so. Pursuant to Penal Code (PC) 46.035 and A&M-Commerce Rule 34.06.02.R1, license holders may not carry a concealed handgun in restricted locations.

For a list of locations, please refer to the Carrying Concealed Handguns On Campus

The *syllabus/schedule are subject to change.*

document and/or consult your event organizer.

Web URL:
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/34SafetyOfEmployeesAndStudents/34.06.02.R1.pdf

Pursuant to PC 46.035, the open carrying of handguns is prohibited on all A&M-Commerce campuses. Report violations to the University Police Department at 903-886-5868 or 9-1-1.

COURSE OUTLINE / CALENDAR

Week	Date	Topic
1	8/30	– Lecture 1: Introduction & Course Overview – Assignment 1: Course Introduction & Overview
2	9/6	**NO CLASS – Labor Day Holiday**
3	9/13	– Lecture 2: ICS Fundamentals – Part 1: Operation, Design & Vulnerabilities – Assignment 2: ICS Fundamentals – Quiz 1: ICS Fundamentals 1
4	9/20	– Lecture 3: ICS Fundamentals – Part 2: Networking & Industrial Protocols – Quiz 2: ICS Fundamentals 2
5	9/27	– Lab 1: Network Analysis Tools
6	10/4	– Lecture 4: Assessing & Managing Risk – Assignment 3: Risk Identification & Classification – Quiz 3: Assessing & Managing Risk
7	10/11	– Lecture 5: Auditing & Assessing ICS – Part 1: Methodology & Identification – Assignment 4: Auditing & Assessing ICS using CSET – Quiz 4: Auditing & Assessing ICS 1
8	10/18	– Lab 2: ICS Identification & Characterization – Term Paper: Topic Selection
9	10/25	– Lecture 6: Auditing & Assessing ICS – Part 2: System Assessment & Classification – Assignment 5: Vulnerability Identification – Quiz 5: Auditing & Assessing ICS 2
10	11/1	– Lab 3: ICS Vulnerability Identification

The *syllabus/schedule are subject to change.*

Week	Date	Topic
11	11/8	– Lecture 7: Standards & Best Practices for Industrial Security – Assignment 6: Standards & Best Practices for ICS – Lab 4: Open-Source Intelligence – Quiz 6: Standards & Practices
12	11/15	– Lecture 8: Selecting & Implementing Security Controls for ICS – Part 1 – Demonstration: Industrial Networking (optional) – Assignment 7: Term Paper Concept Development (Outline) – Quiz 7: Selecting & Implement Security Controls 1
13	11/22	– Lecture 9: Selecting & Implementing Security Controls for ICS – Part 2 – Demonstration: Industrial Firewalls (optional) – Assignment 8: Selecting Security Controls using NIST SP 800-82 Baselines – Quiz 8: Selecting & Implementing Security Controls 2
14	11/29	– Lab 5: ICS Risk Analysis & Security Controls Selection
15	12/6	– Term Paper Presentations
16	12/13	– Final Examination

Note: The right to modify the presentation order of materials is reserved. Course progress will be based on observed progress, feedback, and suggestions from students. All material will be covered, but in the event some topics require additional time, others will be condensed to maintain schedule.