ECE 8498: Cyber-Physical System Security

Class Meetings

Sections 8498-001, 8498-DL1: Tuesday, 6:10-8:50PM, CEER 307

Instructor

Name: Dr. James Solderitsch

Office location: Tolentine Hall Rm 404

Office phone number: (610) 519-4975; Cell phone number: (484) 612-5500

Email: james.j.solderitsch@villanova.edu

Office Hours

Wed. 11am-12pm, Thurs. 4:00 pm – 5:00 pm, other times by appointment (Zoom Teleconferencing Enabled)

Course Objectives

This course will cover the principles and techniques used to engineer secure Cyber-Physical Systems (CPS) in both an industrial setting like Industrial Control Systems (ICS) as well as in a consumer setting where the term Internet of Things (IoT) is often used.

Topics to be covered include:

- Relationships between devices, networks and applications for CPS/ICS/IoT
- Primary CPS processes: Monitor, Control, Optimize, Automate
- Differences between industrial scale, processes and devices compared to consumer level scale
- Importance of Data Modeling, Data Analytics, Device and Application connectivity, Application Development and Enterprise Integration
- Hands-On development of secure IoT Applications using one or more commercial platforms that involve both simulated and real devices
- Attack and Defense labs and exercises for CPS and IoT
- Emerging Security Standards for CPS and IoT
- Engineering practices and guidance for implementing secure CPS and IoT systems
- Case Studies of IoT and CPS exemplary systems and their security properties

There will be some programming concepts covered in the course as we look at CPS and IoT systems, but I will not require a lengthy programming project or coding-heavy assignments. So, reading awareness of Java/Javascript/C/Python code and even some familiarity with operating system and networking concepts

would be nice, but I will not make programming details or construction part of student submissions unless they elect to take that on as part of their final project.

Grading Policy

Your final grade will be determined based on a percentage score out of 400 points where the points will be based on the following course activities:

- Completion of PTC University course from PTC covering ThingWorx and IoT: 35 points (in 2 parts)
- Completion of 2 labs based on the CybatiWorks Power System model featuring a Raspberry Pi and custom PCB board; first lab (basic setup): 10 points; second lab (ICS attack and defense) based on wizard configuration: 25 points for a total of 35 points
- Ladder Logic Assignment: 10 points
- CybatiWorks VM Blackbox Exercise: 30 points
- Completion of Raspberry Pi/Sense Hat development sequence using a TBD Cloud IoT platform: 35 points (in 2 parts)
- Assignment TBD: 20 points
- Midterm Exam: 30 points
- VoiceThread Test Comment: 5 points
- Recorded Presentation on IoT/IIoT/CPS research topic selected by student (not ICS-based if student has completed ECE 8485) OR a hands-on report/demonstration/video of a CPS related project. Submitted as VoiceThread posting: 50 points
- Peer review of 2 Presentations as VoiceThread comments: 20 points (10 per review)
- Final Exam: 60 points
- Yellowdig participation: 70 points; this will be tracked week by week

The scale used to assign letter grades is:

Letter Grade	Numerical Grade	Letter Grade	Numerical Grade
A	94 to 100	C	73 to 76
A-	90 to 93	C-	70 to 72
B+	87 to 89	F	Less than 70
B	83 to 86		
B-	80 to 82		
C+	77 to 79		

Attendance

The following paragraph on attendance, along with the list of excused absences, comes from the College of Engineering and is a required element of the syllabus.

Where possible, students should inform their instructors if they plan to be late or absent from class. In all cases, students should be prepared to provide documentation to petition for *excused* absences to the appropriate Associate Dean. The form for requesting an *excused* absence can be found here (http://www1.villanova.edu/villanova/engineering/resources/policies/forms/studentAbsence.html). Excused absences do not count toward a failure in the course for first year students. Absence from class does not release the student from work assigned. Students who miss an in-class obligation (exam, presentation, etc.) due to an excused absence will not be penalized - the instructor may offer a make-up test, arrange an alternative time for a presentation, exempt a student from the assignment, or provide another arrangement.

The University's list of excused absences for all students includes the following:

- participation in NCAA athletic competitions
- participation in special academic events (e.g., conferences, field trips, project competitions)
- participation in official university business (e.g., student representatives attending meetings related to university governance)
- attendance at significant events involving the immediate family (e.g., funerals, weddings)
- religious holidays - see the University's policy on Religious Holidays
- college-approved participation in placement activities (e.g., job interviews, graduate school interviews, attending job fairs)
- documented serious illness or disability (see below how to document)

This course is available as both an in-class section (001) offered CEER 307 and as a distance learning section (DL1). DL1 students are encouraged, if their schedule permits, to attend in person at Villanova. In-class students may elect to attend the class remotely just like the DL1 students. However, it is highly recommended that students keep up with the class on a weekly basis. If circumstances, such as a work assignment or illness, cause a student to miss the weekly class, it is expected that an email is sent to the instructor documenting the nature and length of the class disconnect. Assignments will have due dates and normally a student is expected to complete all assignments on or before the posted due date. Please review the Deadlines section later in this syllabus.

Students are expected to (virtually) attend every class. Slides used in class and saved on Blackboard may have some of the material covered, but not all or even most. Students may contribute insightful information during class that you can learn from. **You are responsible for everything covered in class, regardless of whether the material is addressed in the readings or handouts or on Blackboard.**

Course Materials

There are no required course materials other than those presented or identified in class and these will be provided as resources on the Blackboard site for the course.

Various sources of information on Cyber-Physical Systems and the Internet of Things with an emphasis on Security will be provided and used as reference material.

Materials and even hardware from forward-looking vendors will be included and provided when they support concepts important to the course: robotics, UAVs, sensors and actuators. This material will be used to support student projects and in-class hands-on presentations.

Academic Integrity

The College of Engineering is committed to creating an environment of academic integrity and ethical decision-making that we hope is reflected in the actions of our students and graduates. As Villanova students, integrity is central to the University mission. As engineers, our code of conduct requires us to place honor and integrity at the forefront of everything we do. As engineering students, it is expected that you will begin to adopt these values and instill them into your work habits. Students violating the academic integrity policy will receive a zero on that assignment or exam and the violation will be reported to the Associate Dean for Academic Affairs.

The University's academic integrity policy can be found here: https://www1.villanova.edu/villanova/provost/resources/student/policies/integrity.html.

The College of Engineering has adopted the following exam guidelines:

- Students must arrive before the start of the exam. Under exceptional circumstances a student may need to arrive late, but he/she can enter the exam no later than 5 minutes after the start of the exam.
- All cell phones must be turned off and stored away until the student exits the exam room.
- The official Villanova class attendance policy must be followed when requesting excuses for absences or lateness to an exam.
- Each student must write and sign the following statement, "*I have neither given nor received any unauthorized assistance in the completion of this exam.*"

The statement given above about exam protocol is meant for in-class exams that will not be part of this course.

Don't be evil

The knowledge you gain in class is for educational purposes only. You may gain powers in this class that you are duty and honor bound not to misuse. You will promise not to scope out, attack, subvert or disrupt Villanova ECE, Villanova, corporate, county, US state or federal computer systems. US State and Federal law does not take these things lightly - prison and $10,000s of fines. Foreign students will probably lose their visa and be deported. Be careful with what you do and where and how you do it.

Students with Disabilities

It is the policy of Villanova to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability please contact me after class or during office hours to make arrangements.

If you have a non-physical disability you need to register with the Learning Support Office by contacting 610-519-5176 or at learning.support.services@villanova.edu as soon as possible. Registration is needed to receive accommodations.

The Office of Disability Services collaborates with students, faculty, staff, and community members to create diverse learning environments that are usable, equitable, inclusive and sustainable. The ODS provides Villanova University students with physical disabilities the necessary support to successfully complete their education and participate in activities available to all students. If you have a diagnosed disability and plan to utilize academic accommodations, please contact and register with Gregory Hannah, advisor to students with disabilities @ 610-519-3209 or visit the office on the second floor of the Connelly Center.

Schedule

The following calendar of the course is ***VERY*** tentative. Tuesday April 16 is officially a class day although Thursday April 18 is not. For now, we will keep April 16 as an open date. It may be used in place of a weather impacted class.

DATES AND TOPICS ARE SUBJECT TO CHANGE

January 15:	Overview of Course; PTC IoT University Introduction; 8498 Lab Equipment First Look; First PTCU assignment; ICS Security Concepts
January 22:	IoT Concept Summary from PTCU course; PTCU course tools; Second PTCU Assignment; Assembly of Power System Model; Power System Model First Assignment

January 29:	Defcon 26 ICS slides, Power System Model Second Assignment; Ladder Logic Hands-On;
February 5:	More on ICS security; CybatiWorks Blackbox Assignment; Hands-On with other Cybati ICS models
February 12:	CPS Edge to Cloud concepts using IoT Cloud; Introduction to Node-Red; First Sense Hat Assignment with Raspberry Pi
February 19:	More with Node-Red; Second Sense Hat Assignment with Raspberry Pi
February 26:	More IoT/CPS/Cybati platform introductions and explorations: e.g. Hackster.io; Midterm Exam;
March 12:	Contiki IoT OS; Contiki NG; SensorTag programming; Course Research or Hands-On Presentation Topic Selected; TBD Assignment;
March 19:	Thingsquare SDK, based on Contiki; SensorTag programming with SDK; Research/Demo Presentation Guidelines
March 26:	CPS Security: deeper dive; CPS networks and communications mechanisms; Other CPS Platforms; Critical Infrastructure Security Awareness; Research Presentation due
April 2:	More on CPS Security: device and network monitoring; Still more CPS platforms; Critical Infrastructure Security Actions; Presentation Peer Review comments due
April 9:	Smart Manufacturing with PTC ThingWorx: Sigma-Tile exploration; Cybati Manufacturing Model
April 23:	Blockchain Concepts. Blockchain technology and CPS Security. Supply Chain Application
May 2:	Semester Wrap-Up. Final Exam

Assignments

Assignments in this course will be distributed throughout the course and typically be due within 1 to 2 weeks from the class at which they are reviewed. Some of them will require hands-on activity using several IoT platform components. Information on acquiring any equipment needed to complete the assignments will be given during class. Detailed preparation and submission instructions will be provided when the assignment is made available.

PTC IoT University Foundations Course

A link to enroll in the IoT University course will be provided in the first class. You will complete this course and provide two assignment submissions showing progress and then completion of the course. Hands-on with a PTC/ThingWorx IoT academic platform is part of this assignment.

Raspberry Pi with Sense Hat Using Node-Red

This two-part assignment will show how to connect the Raspberry Pi with the Sense Hat sensor board to the internet. The assignment is based on some IoT-Cloud-provided tutorials but configuration changes have

occurred that will be documented in resources provided by the instructor. You can use the same Raspberry Pi that is included in the Power System Model kit.

Raspberry Pi Power System ICS Model

For those students who completed the ICS Security course (ECE 8485), these assignments will be familiar and perhaps somewhat repetitive. But, CybatiWorks has produced a modified Virtual Machine that will be used to interact with a brand new model.

Semester Research Project

The domain of Cyber-Physical Systems and Security is large and complex. You will be expected to identify a topic of interest and then explore that topic and prepare a 10 to 15-minute recorded presentation that presents your findings. If you wish, you can continue with hands-on exploration of the lab equipment or acquire and experiment with your own equipment resources. This presentation will be due by the March 28 class.

Exams

While there is no text book for this course, we will be covering a broad range of material. You will be asked to provide answers to questions based on this material at the middle and end of the semester. You should expect the questions to be sufficiently detailed that several sentences or a short paragraph will be sufficient to allow you to provide a correct response. The number of points allocated to these exam assignments is relatively low because you will be engaged with many hands-on activities throughout the semester.

TBD Assignment

Cyber-Physical Systems and their Security is an area where dynamic changes and opportunities for breach and compromise are frequently in the news. You **may** be asked to watch/review a resource (perhaps a webinar presentation from SANS or an innovative vendor in the CPS area) and then provide a written reaction to what you learn by reviewing the resource. There might be specific areas that you will asked to cover in your submission for this assignment or a more general personal reaction may be invited.

Deadlines

Late submission of any assignment may be subject to a deduction of 2 percentage points from the grade for the late assignment per business day per offense. For example, for an assignment worth 10 points, 0.2 points could be deducted per day. This penalty will be deducted from the assignment grade as determined by the other course requirements.

Prerequisites

There is a catalog-noted pre-requisite of ECE 8485: Industrial Control Systems Security for this course. I have been inclined to waive this for early offerings of the course. But that means that some basic ICS security content that is needed for understanding the larger landscape of Cyber-Physical Systems will be included. This will not be new content for students who have completed ECE 8485 but it will be worthwhile as review material.