CYBER SECURITY ENGINEERING (CYSE)

100 Level Courses

CYSE 101: *Introduction to Cyber Security Engineering.* 3 credits.
Provides comprehensive introduction to the principles, applications, and practice of cyber security engineering. Students learn the basic concepts and terminology of cyber security and how cyber security is commonly addressed after the design and implementation phases. Students are introduced to the systems engineering and design processes and learn to integrate and apply cyber security tools and techniques in these processes. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 130: *Introduction to Computing for Digital Systems Engineering.* 3 credits.
The course introduces students to programming in the context of Systems Design process. Students learn to take a systems perspective when approaching problems and designing solutions, how the structure and behavior of a system is modeled using SysML, and to implement the system model using programming techniques in Python. The course explores various Python modules (standard library and 3rd Party) that extend the basic language functionality in useful ways, in particular, for model based systems engineering. The students apply their programming skills to solve commonly encountered Task Automation, Data Mining, Cleansing, and Transformation. Course emphasizes the use of appropriate Web Services APIs and technologies commonly encountered in Data Analytics and AI to find, access, and analyze available data and datasets. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts. Equivalent to SYST 130.
Mason Core: Mason Core (All), Info Tech & Computing (http://catalog.gmu.edu/mason-core/)

Recommended Prerequisite: Passing score on the math placement test for MATH 113.

Registration Restrictions:
Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

200 Level Courses

CYSE 211: *Operating Systems and Lab.* 3 credits.
Addresses basic issues such as virtual memory, kernel and user mode, system calls, threads, context switches, interrupts, interprocess communication, coordination of concurrent activities. May also address: concurrency, processes and multi-threading, context switching, synchronization, scheduling, and deadlock. Memory management, dynamic memory allocation, address translation. Management of file systems, storage devices, directories, protection, scheduling and crash recovery. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: CS 222[C] and CYSE 101[C].
[C] Requires minimum grade of C.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 230: *Computer Networking.* 3 credits.
Introduces network concepts; OSI reference model and layering; data coding; analog/digital communications review; physical layer and data link control; Data Link Layer Control protocols; flow control; error control; link management; common link protocols. LAN and WAN; connection-oriented and connectionless packet switching; circuit-switched networks and control signaling; congestion control and traffic management; transport layer client-server model; domain name systems, routing methods. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: ((CS 112[C], 112[XS], 109[C] or 109[XS]) and (CYSE 101[C] or 101[XS]) and (MATH 113[C] or 113[XS])).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

300 Level Courses

CYSE 304: *Cyber Security in Logic Design and Digital Systems.* 3 credits.
This course provides basic cyber security concepts in logic design and digital systems. Topics covered include an overview of digital concepts, coding conversion and its applications in digital systems, programmable logic devices, and memory expansion basics. An introduction to microprocessors and digital signal processing will be presented. Integrated circuits (ICs) technologies will be discussed. Security issues related to logic design, including reverse engineering, IC counterfeiting, and malicious tampering, will be addressed. Methodologies for logic design security regarding logic locking in which only authorized persons can access the circuit's original functionality will be handled. Design projects using simulation and hardware implementation based on Field Programmable Gate Array (FPGA) boards will be presented. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to three attempts.
Registration Restrictions:
Required Prerequisites: (ECE 301[C])(or (ECE 231[C] and 232[C])).

[C] Requires minimum grade of C.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 395: *Cyber Security Engineering Internship.* 3 credits.
Students will participate in experiential learning in an industrial setting. Students must identify work opportunity and seek approval from the internship coordinator prior to registering. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the degree for a maximum 6 credits.
Registration Restrictions:
Required Prerequisites: ((CS 112[C], 112[XS], 109[C] or 109[XS]) and (CYSE 101[C] or 101[XS]) and (MATH 113[C] or 113[XS]) and (CYSE 230[C] or 230[XS])).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Schedule Type: Internship

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

400 Level Courses

CYSE 411: *Secure Software Engineering.* 3 credits.
This course provides a foundation for building secure software by applying security principles to the software development lifecycle. Topics covered include: security in requirements engineering, secure designs, risk analysis, threat modeling, deploying cryptographic algorithms, defensive coding, penetration testing, fuzzing, static analysis, and security assessment. Students will learn the practical skills for developing and testing secure software. Notes: This course may be of interest to students specializing in software aspects of cyber security engineering. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (CS 222[C] or 222[XS]) or ((CDS 130[C] or 130[XS]) and (SYST 230[C] or 230[XS])).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 421: *Industrial Control Systems Security.* 3 credits.
Provides an introduction to industrial control systems (ICS). Covers fundamental concepts of control loop and its main components. Human-Machine Interface (HMI) and displays. Remote measurements through networks or through telemetry. Diagnostic and maintenance utilities. Input-Output servers. Data historian utility. SCADA systems. ICS Security. Connectivity of the control system network to other networks. Possible security threats. Vulnerability assessments. Multilayer defense strategies. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: ((CYSE 230[C] or 230[XS]) and (ECE 301[C], 301[XS] or L301 or (ECE 231[C] and 232[C]))).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 424: *Embedded and Real Time Systems.* 3 credits.
Presents design methodology, principles and practice for the development of real-time embedded systems and their application to robotics, mechatronics, sensing, signal processing, and control. They include automated sensors, switches and PLCs. Topics include system decomposition, multi-tasking, task communication and synchronization, system modeling, time analysis, principles of filter and controller implementation, 'fuzzy' engineering, and multimicrocontroller systems. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (ECE 301[C], 301[XS] or L301 or (ECE 231[C] and 232[C])).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 425: *Secure RF Communications.* 3 credits.
Reviews current systems of Radio Frequency (RF) communications and related cyber security issues. This course focuses on security issues in wireless networks, such as cellular networks, wireless LANs, Bluetooth, NFC, RFID, mobile security, anti-jamming communication, and physical layer security. The course will first present an overview of wireless networks, then focus on attacks and discuss proposed solutions and their limitations. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts. Equivalent to ECE 425.
Registration Restrictions:

Required Prerequisites: ((CS 222[C], 222[XS], ECE 240[C], 240[XS], CS 262[C] or 262[XS]) and (ECE 465[C], 465[XS], CYSE 230[C], 230[XS], CS 455[C] or 455[XS]) and (MATH 125[C], 125[XS], ECE 231[C] or 231[XS])).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major, minor, or concentration in Computer Engineering, Computer Science, Cyber Security Engineering, Electrical and Computer Engr or Electrical Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 430: *Critical Infrastructure Protection.* 3 credits.
Consists of a four week lecture course followed by ten weekly seminars presented by students. The lecture part provides a description of US Designated Critical Infrastructure Sectors and a corresponding list of federal sector specific agencies (SSAs). Each student selects a sector, develops and presents a seminar talk on critical cyber security issues involved in a given sector. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (SYST 205[C], 205[XS], CYSE 205[C] or 205[XS]).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 445: *System Security and Resilience.* 3 credits.
Focuses on modeling and evaluation of the engineering systems that are expected to operate in a contested cyber environment. Covers architectures and modeling, uses a variety of techniques, establishing measures of performance that are relevant to the domain of operation, evaluating the security or vulnerability of the system to cyber exploits, and then assessing its resilience. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: ((ECE 301[C], 301[XS], L301 or CYSE 301[C] or (ECE 231[C] and 232[C])) and CYSE 230[C] and 450[*C]).
[*] May be taken concurrently.
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 450: *Cyber Vulnerability Lab.* 1 credit.
Lab for CYSE 445. Provides hands-on experience in security issues of network systems. Issues in ethical hacking, penetration testing, forensics and incident handling and response will be discussed. Notes: This is a hands-on lab course, with short lecture introductions. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (CYSE 445[*C] or 445[XS]).
[*] May be taken concurrently.
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Laboratory

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 460: *Power Systems and Smart Grid Security.* 3 credits.
Covers fundamentals of power systems; basics of electricity, electricity generation, economics of supply and demand, and electricity market operations in regulated and deregulated environment. The other part of the course will cover Smart Grid and its impact on the energy industry. Also includes Energy policy modeling and analysis. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 461: *Power Grid Security.* 3 credits.
Overview of integrating smart grid into the current system. Includes the seven domains (bulk generation, transmission, distribution, customer, operations, markets, and service providers) as well as the electrical and communication interfaces that connect the layers and domains. Focuses on monitoring equipment in the smart grid. Provides an overview of security principles and approaches for applying them to the smart grid. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisite: CYSE 460[C].
[C] Requires minimum grade of C.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 462: *Mobile Devices and Network Security.* 3 credits.
Embedded security features of hand-held wireless devices. Data link layer encryption and authentication protocols applied in mobile devices. Security factors in the decisions on configuring wireless mobile devices and network infrastructure. Robust cryptography that is needed to attain the highest levels of integrity, authentication, and confidentiality. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (CYSE 425[C], 425[XS], ECE 425[XS] or 425[C]).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major, minor, or concentration in Computer Engineering, Cyber Security Engineering or Electrical and Computer Engr.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 465: *Transportation Systems Design.* 3 credits.
Discusses common elements and differences among problems that occur securing road, rail, air and sea transportation systems. Covers threats to control systems. Introduces control measures. Discusses past, present and future of in-vehicle and on-road safety systems, and cyber threats to emerging autonomous cars. Analyzes cyber threats to aviation and sea transportation security and available countermeasures. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: SYST 230[C] or 230[XS].
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Students with a class of Freshman or Sophomore may **not** enroll.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 467: *GPS Security.* 3 credits.
A review of Global Navigation Satellite System (GNSS) is presented. The GPS system and its components are discussed. Examine the digital code structure of course/acquisition (C/A) code and Precise (P) code, GPS modernization and the key types of GPS measurements. The GPS satellite orbit and the broadcast ephemeris are described. Discuss the errors and biases that affect the GPS measurements. GPS spoofing and jamming vulnerabilities are addressed. Substantial increase in GPS security level including signal coding and secure GPS antenna design using new materials is discussed. Integration of GPS with other complementary systems is illustrated. GPS applications in various fields are introduced. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (CYSE 425[C] or 425[XS]).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 470: *Human Factors and Cyber Security Engineering.* 3 credits.
This course explores the human factor in cyber security engineering. The focus is on understanding human performance characteristics and limitations, and the various research, design, and evaluation methods needed to address them when engineering secure systems. Topics include, for example, perception, cognition, memory, situation awareness, decision making, stress, automation, and human-computer display and interaction design principles. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: ((SYST 205[C] or 205[XS]) and (STAT 344[C], 344[XS], 346[C] or 346[XS])).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 476: *Cryptography Fundamentals.* 3 credits.
Covers basic concepts of cryptology, types of cryptosystems, security services, and key management. Gradually introduces mathematical background required for understanding cryptography. Discusses modern secret-key stream and block ciphers, modes of operation, public key cryptosystems (RSA, elliptic curve, and post-quantum cryptography), hash functions, message authentication codes, and digital signature

schemes. Covers key cracking machines, side-channel attacks, and fault attacks. Discusses popular cryptographic modules, such as True Random Number Generators and Physical Unclonable Functions, used for key generation and device authentication. Introduces educational and public domain software implementing modern cryptographic algorithms. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts. Equivalent to ECE 476.
Registration Restrictions:
Required Prerequisites: (ECE 301[C], 301[XS], 231[C], 231[XS], 331[C] or 331[XS]).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Computer Engineering, Computer Science, Cyber Security Engineering or Electrical Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 477: *Intrusion Detection.* 3 credits.
The objective of this course is to provide an in depth introduction to the science and art of intrusion detection. The course covers methodologies, techniques, and tools for monitoring events in computer systems or networks, with the objective of preventing and detecting unwanted process activity and recovering from malicious behavior. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: SYST 230[C] or 230[XS].
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Students with a class of Freshman or Sophomore may **not** enroll.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 478: *Cyber Security Audit and Compliance.* 3 credits.
Fundamental concepts of the Cyber Security Compliance and Testing process. This will revolve around defining a control framework, the attendant control objectives and the reporting system for an organization. Covers the process of creating a control structure with goals and objectives, audit a given cyber infrastructure against it, and if found inadequate, establish a systematic remediation procedure. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: CYSE 421[C] or 421[XS].
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 479: *Methods of User Authentication.* 3 credits.
Discusses limitations of passwords and PINs and introduces alternatives. Covers user authentication based on security tokens and smart cards. Introduces basics of biometric systems, based on information such as fingerprints, facial features, iris, and voice. Discusses the use and security of electronic ID cards and passports. Covers methods of distinguishing human from internet bots over the network, such as CAPTCHA's. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: (CYSE 211[C] and (CYSE 301[C], ECE 301[C] or L301 or (ECE 231[C] and 232[C])) and CYSE 230[C] and (CS 222[C] or SYST 230[C])).
[C] Requires minimum grade of C.

Students with a class of Freshman or Sophomore may **not** enroll.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 480: *Reverse Software Engineering.* 3 credits.
Introduces various types of malicious software (malware). Discusses malware analysis using virtual machines, sandboxes, process monitors, packet sniffers, de-obfuscation, etc. Introduces hardware Trojans and other forms of malicious hardware. Discusses prevention techniques at the design, fabrication, and post-fabrication level. Introduces various countermeasures against malicious software and hardware. The course has a lab with Windows and Android operating systems. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Recommended Prerequisite: 60 credits towards BS in Cyber Security Engineering.

Registration Restrictions:
Required Prerequisites: ((CYSE 211[C] or 211[XS]) and (ECE 301[C], 301[XS] or L301 or (ECE 231[C] and 232[C]))).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 491: *Engineering Senior Seminar.* 3 credits.
This course covers a variety of responsibilities of cyber security engineers including: engineering ethics, government policies, laws and regulations affecting cyber security engineering, industry practices, entrepreneurship. Effective technical communications. Incorporates global implications of cyber security engineering. Speakers include faculty, invited guests from industry and government, as well as students. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Mason Core: Mason Core (All) (http://catalog.gmu.edu/mason-core/)

Specialized Designation: Writing Intensive in Major

Registration Restrictions:
Required Prerequisites: ((CYSE 411[C], 411[XS], 421[C], 421[XS], 425[C], 425[XS], MATH 213[C] or 213[XS]) and (CYSE 492[*C])).
[*] May be taken concurrently.
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 492: *Senior Advanced Design Project I.* 3 credits.
First semester of a two semester capstone course in the Cyber Security Engineering program. Development of a design project by a team of students. Conception of the project and determination of its feasibility. Work includes developing preliminary design and implementation plan. Projects will aim at the integration of the technical material learned in several courses and incorporation of industry input. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Required Prerequisites: ((CYSE 411[C], 411[XS], 425[C], 425[XS], 476[C] or 476[XS]) and (CYSE 491[*C])).
[*] May be taken concurrently.
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 493: *Senior Advanced Design Project II.* 3 credits.
Second semester of a two semester capstone course in the Cyber Security Engineering program. Project includes designing a cyber-physical security system, writing required software, assembling hardware if needed, conducting experiments or studies, and testing the complete system. Requires oral and written reports during project and at completion. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Mason Core: Mason Core (All), Mason Apex (http://catalog.gmu.edu/mason-core/)

Registration Restrictions:
Required Prerequisites: (CYSE 492[C] or 492[XS]).
[C] Requires minimum grade of C.
[XS] Requires minimum grade of XS.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 498: *Independent Study in Cyber Security Engineering.* 1-3 credits.
Research and analysis of selected problems or topics in Cyber Security Engineering. Topic must be arranged with instructor and approved by department chair before registering. Notes: May be repeated if topics substantially different. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the term for a maximum 6 credits.
Specialized Designation: Topic Varies

Registration Restrictions:
Students with a class of Freshman or Sophomore may **not** enroll.

Enrollment is limited to students with a major in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Independent Study

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 499: *Special Topics in Cyber Security Engineering.* 3 credits.
Special Topics in the Cyber Security Engineering area, with different content in different terms. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the term for a maximum 12 credits.
Specialized Designation: Topic Varies

Recommended Prerequisite: 60 credits towards BS in Cyber Security Engineering.

Registration Restrictions:
Enrollment limited to students with a class of Junior Plus, Junior, Senior Plus or Senior.

Enrollment is limited to students with a major, minor, or concentration in Cyber Security Engineering.

Students with the terminated from CEC major attribute may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Undergraduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

500 Level Courses

CYSE 521: *Industrial Control Systems Security.* 3 credits.
Provides an introduction to industrial control systems (ICS) at a Graduate level. Covers fundamental concepts of control loop and its main components.Human-Machine Interface (HMI) and displays. Remote measurements through networks or through telemetry. Diagnostic and maintenance utilities. Input-Output servers. Data historian utility. SCADA systems. ICS Security. Connectivity of the control system network to other networks. Possible security threats. Vulnerability assessments.Multilayer defense strategies. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 550: *Cyber Security Engineering Fundamentals.* 3 credits.
This is the introductory graduate course in Cyber Security Engineering. It is a technical course that provides the required foundations for successful completion of the MS CYSE program. The course introduces key subjects in the area, such as engineering systems and cyber security problems in engineering; cyber security design; introduction to Cryptography; system and network security; identity management; adversarial modeling; vulnerability assessment; and industrial control and manufacturing security. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 570: *Fundamentals of Operating Systems.* 3 credits.
Operating system design and implementation as it relates to management and interaction of processor, memory, files, and I/O devices. Includes security considerations and a review of data structures, programming concepts, and computer systems architecture. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 580: *Hardware and Cyber Physical Systems.* 3 credits.
Covers computer architecture and hardware to support subsequent cyber-physical systems modules. Introduces cyber-physical systems as an integration of physical processes, computation, and networking. Discusses modeling and simulation of cyber-physical systems, system design, and implementation. Covers security issues in cyber-physical systems and applications selected from infrastructure, energy, transportation, robotics, manufacturing, and communications domains. Students study and build cyber-physical systems. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 587: *Cyber Security Systems Engineering.* 3 credits.
This course addresses cyber security from the standpoint of systems engineers. It introduces core principles for the design and management of resilient and robust systems throughout their complete lifecycle. Topics include but are not limited to lifecycle assurance of systems, risk analysis, models for secure systems development and management, gap analysis, quantitative methods for cyber security, and special topics in cyber security. The course also covers distinct technologies for assessing system vulnerabilities, measuring and modeling risk, reducing uncertainty in risk management, and others. Target audience consists of engineers who want to expand their skill sets to better align with the demands of current cyber security jobs, as well as those who intent to work on cyber security research. Cyber security professionals would also benefit from the course by being exposed to a systems engineering, holistic perspective on cyber security design, development, and management. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit. Equivalent to CYSE 787, SYST 687, SYST 787.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

600 Level Courses

CYSE 610: *Networks and Cyber Security.* 3 credits.
Introduction to architectures and protocols of computer networks and concept of packet switching. Topics include ISO standard layer model, physical interfaces and protocols, data link control, multi-access techniques, packet switching, routing and flow control, network topology, data communication subsystems, error control coding, local area network, wireless communications, satellite packet broadcasting, packet radio, interconnection of packet-switching networks, network security and privacy, and various examples of computer networks. Security threats and countermeasures are addressed in detail to include firewalls, intrusion detection and prevention, physical security, and network monitoring. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Required Prerequisite: CYSE 550[B-].
[B-] Requires minimum grade of B-.

Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Laboratory, Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 630: *Cyber Risk Analysis and Advanced Tools.* 3 credits.
This course addresses cybersecurity risk analysis from the standpoint of systems engineers. It introduces core principles for modeling and measuring uncertainty and risk in the secure development lifecycle and risk. Topics include but are not limited to risk analysis, quantitative and qualitative methods for cybersecurity, risk models and frameworks, and support tools (Bayesian, Shafer-Dempster, and Fuzzy systems for probabilistic reasoning). The course also covers distinct technologies for assessing system vulnerabilities, measuring and modeling risk, reducing uncertainty in risk management, and applying engineering concepts to cybersecurity. The target audience consists of engineers who want to expand their skill sets to better align with the demands of current cybersecurity jobs and those who intend to work on cybersecurity research. It requires a consolidated skill, at least in one programming language (such as Java, C++, Python). Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: (CYSE 587) OR (SYST 687) OR (CYSE 787)

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 640: *Wireless Network Security.* 3 credits.
This course provides an in-depth understanding of the security challenges and opportunities associated with key-enabling wireless networking technologies, such as WiFi, 5G, Bluetooth, etc. It covers the latest security mechanisms, trends, and practices for securing wireless networks. It has a strong focus on the security risks and challenges associated with wireless networks, including jamming, spoofing, man-in-the-middle attack, MAC-layer misbehavior, cross-layer attacks, and others. Students are presented with a detailed account of more advanced concepts on 5G wireless networks, such as network slicing, Open Radio Access Network (O-RAN), and Software-defined networking (SDN). Various security measures and technologies used to secure wireless networks are explored, including wireless encryption protocols, wireless access control methods, anti-jamming and low probability of detection/intercept (LPD/LPI), wireless intrusion detection and prevention systems. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: CYSE 610

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 650: *Topics in Cyber Security Engineering.* 3 credits.
Topics not covered in department's regular Cyber Security Engineering offerings. Course content may vary each semester depending on instructor and the perception of students' needs. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the term for a maximum 6 credits.
Specialized Designation: Topic Varies

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 670: *Secure Design of Connected and Automated Vehicles.* 3 credits.
This research oriented course addresses the research and engineering challenges faced in designing and implementing connected automated vehicles. These involve multiple aspects of sensing, recognition, control and communication aspects for vehicles and road-side infrastructure. Two important aspects of automated and connected vehicles are the need to minimize traffic delays and congestion while being cognizant and accommodating the needs of pedestrians, bicyclist and other entities that need to share the roads and roadside spaces. In addition, special needs

such as providing the right of way for emergency vehicles and traffic arrangements around special events and parking in congested cities are issues that needs to be addressed in a comprehensive framework for connected automated vehicles. The class will discuss current topics related to communication standards such as 5G/DSRC, basic Safety Message Systems etc., and how they would work with existing traffic signals and vehicular contr Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 680: *Advanced Manufacturing Automation Security.* 3 credits.
This course explores the application of Cyber Security concepts in support of advanced manufacturing. The focus is on techniques applicable to Industrial Automation and Control Systems (IACS) against threats to security through unexpected situations, activities or occasions, or through consider assault. Topics include cyber-physical security, establishing causality between cyber execution, physical production, and energy consumption for intelligent efficiency, and detection of cyber threats based on physical process anomalies in advanced manufacturing systems. The course will also cover advanced equipment and product management functions, distributed vulnerability discovery, causality analysis and attack defenses, and Cyber-physical ledger infrastructure. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 681: *Secure Energy Efficient Supply Chains.* 3 credits.
This course explores the application of Cyber Security concepts to secure supply chain networks and enable data-intensive energy efficiency. The focus is on techniques that enable supply chains in diverse sectors to employ IIoT devices while avoiding a substantial increase of its attack surface, enabling pervasive data collection to support automation, integration, and process enhancements. A special attention will be given to the criteria and metrics for evaluating supply chains with respect to their energy efficiency and carbon footprint reduction. Topics include Secure IIOT architectures, e-ROI, carbon footprint assessment, modeling and simulation of supply chain security, cyber-physical identification, tracking, and verification of parts and products in a uniform, hierarchical fashion, digital twins, counterfeit detection, product recall, and supply chain re-routing for higher energy efficiency. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit. Equivalent to SYST 681.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 682: *Formal Methods for Cyber Physical Systems Security.* 3 credits.
Formal techniques applied to computer security provide a reliable way of demonstrating that a system is immune to entire classes of attacks (provided the assumptions of the models are satisfied). This is a stark contrast with the more general approach of ruling a system as secure until an attack proves otherwise. This course explores the various ways in which formal methods can be applied to the security of cyber-physical systems. Emphasis is given to CPS used in advanced manufacturing industries and their associated supply chain networks. Topics include formal specification languages for security properties, security analysis utilities, domain-specific security concerns, translating informal requirements to formal specifications in languages such as AADL, satisfiability solvers (SAT), satisfiability modulo theories (SMT), real-time model checking, verification of system requirements, and case studies of formally verified secure systems. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 683: *Reverse Engineering Industrial Automation.* 3 credits.
This course presents fundamental, systems-level concepts for developing an understanding of the underlying functionality of an industrial system without a prior access to the system's design specifications. Considers generalized approaches to developing a set of specifications for a complex system through orderly examination of specimens of that system. Illustrates procedures for identifying the system's components and their interrelationships. Demonstrates methods for creating representations of the system in another form or at a higher level of abstraction. Presents fundamental definitions for forward engineering, reverse engineering, design recovery, restructuring and reengineering. Case studies from several domain areas will be presented to include: integrated circuit (IC) and circuit board analysis, communications protocol analysis, software disassembly, and programmable logic verification. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:

Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 685: *Unmanned Aerial Systems Security.* 3 credits.
This course provides engineers with a background in the essential components and operation of Unmanned Aerial Systems (UAS), related counter measures and protective measures. It introduces core principles for the safe and secure operation of UAS, especially in the C4I context. Topics are focused on UAS components, characteristics, and operational environment, such as weather and radio propagation. The course also covers active and passive detection of UAS, methods to avoid detection and for disrupting UAS operations, such as electromagnetic interference and cyberattacks, as well as measures against these methods, such as RADAR and IR stealth concepts. Finally, this course brings a holistic view of UAS security and its future trends. The target audience consists of engineers interested in planning, designing, or participating in UAS operations from a safety and security standpoint. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: Engineering graduate standing, solid understanding of calculus, statistics, and probability theory

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 689: *Artificial Intelligence Methods for Cybersecurity.* 3 credits.
This course provides engineers with an overview of the core principles of applying ar-tificial intelligence to cybersecurity. It covers approaches for predicting, detecting, and responding to cyber threats using technologies such as Bayesian networks, multi-entity Bayesian networks, search-based methods, decision making, causal learning, reinforcement learning, and others that can be applied to the security of cyber physi-cal systems. It requires familiarity with basic concepts in probability and statistics, discrete mathematics, and optimization algorithms. Programming and software de-velopment skills in languages such as Python and Java are expected, although not at an advanced level. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: CYSE 587

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 690: *Cyber Security Engineering Capstone Project.* 3 credits.
Analysis and design of a complex cybersecrurity-engineered integrated system involving software, hardware and people. Involves application of cyber security engineering principles to the design, implementation and operation of the system. Includes requirements analysis, analysis of design alternatives, assessment of threats, and risk, economical and regulatory considerations. Requires oral and written reports throughout the course. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Required Prerequisites: (SYST 687[B-] and (CYSE 570[B-], CS 571[B-] or 571[XS]) and CYSE 580[B-] and 610[B-]).
[B-] Requires minimum grade of B-.
[XS] Requires minimum grade of XS.

Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Seminar

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 698: *Independent Study and Research.* 3 credits.
Study of a selected area in Cybersecurity EngineeringI under the supervision of a faculty member. A written report is required. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the degree for a maximum 12 credits.
Recommended Prerequisite: Completion of at least 2 MS CYSE core courses

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Independent Study

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

700 Level Courses

CYSE 700: *Research Methodology and Pedagogy in Cyber Security Engineering.* 3 credits.
The course will explore the dynamic intersection of theory and practice in the area of cybersecurity. It will delve into advanced research methodologies, including qualitative and quantitative approaches, ethical considerations, and data analytics specific to cybersecurity contexts. Simultaneously, students will gain insights into cutting-edge pedagogical strategies tailored for cybersecurity education. Students will develop expertise in curriculum design, teaching methodologies, and industry collaboration. The course will prepare students for a future in academia

or industry leadership roles by getting familiar with methodologies in teaching and research in the area of cybersecurity. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). Limited to two attempts.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Activity-Based

Grading:
This course is graded on the Satisfactory/No Credit scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 710: *Advanced Networks and Cyber Security.* 3 credits.
This course will cover advanced theory and practice of secure network design and cybersecurity issues. Topics will include access control mechanisms, computer network protocols, physical interfaces, routing and flow control, wireless communications, network security and privacy, and common cybersecurity threats. In addition, discussions on security primitives such as state-of-the-art firewalls, intrusion detection and prevention, physical security, network monitoring, and cryptography primitives will be explored. Network security research will be emphasized, with students exposed to the latest advances in network security and expected to carry on network security projects and/or work on research papers. The target audience consists of both PhD and advanced MS students with engineering backgrounds. This course will include a semester-long research project on computer network security. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Corequisite: Prior exposure to computer networks.

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 731: *Graphical Models for Cybersecurity.* 3 credits.
This course addresses the use of this knowledge representation paradigm in the general area of cybersecurity from the standpoint of engineers. The first part of the course introduces core principles of graph theory, while providing a basis for understanding the semantics of most graphical methods applied to Cybersecurity. Then, in the second part of the course, probabilistic graphical models are introduced as a key component for applying AI and machine learning techniques to cybersecurity. Topics covered include Bayesian networks and its derivatives, where both its representational features as well as its mathematical and logical quantification aspects are explored. Finally, the course shifts to a wider spectrum of graphical techniques, including but not limited to, attack graphs, evidence graphs, and others commonly used in cybersecurity. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: CYSE 689 CYSE 687

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 750: *Advanced Topics in Cyber Security Engineering.* 3 credits.
Advanced topics not covered in department's regular systems engineering offerings. Course content may vary each semester depending on instructor and the perception of students' needs. May be repeated for credit when topics are distinctly different. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the term for a maximum 6 credits.
Specialized Designation: Topic Varies

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 757: *Cyber Law.* 3 credits.
Technological developments and progress have made cybercrimes (i.e., crimes committed using or targeting a computer) more prevalent, efficient, and cost-effective. Additionally, the rise of novel technologies, such as Artificial Intelligence, poses new challenges for the legal system and society. To understand these challenges, as well as how courts, regulators, and the private sector are responding to them, this course will focus on (1) Substantive computer crimes that involve a computer either as a target or as a medium through which a traditional crime is committed; (2) laws that govern the collection of computerized or digital evidence; (3) regulation of consumer privacy and data protection, including a comparative study of the U.S. and E.U. approaches to privacy regulations; (4) the importance of design for new technologies; and (5) jurisdictional issues from both a U.S. and international perspective. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 760: *Human Factors in Cyber Security.* 3 credits.
This course explores complex human roles in designing resilient/secured systems to meet the products and services necessary for evolving and dynamic technology demands. This research-based course focuses on existing and proposed research spanning studies of the interaction between humans, machines, and technology to develop products and systems that are secure and trustworthy throughout the system engineering process. Topics can cover many fields within Cyber Security Engineering to ensure proper human factors are incorporated (such as design, manufacturing, assembly, measurement, testing, and modeling). The course will address details, including perception, cognition, memory, situation awareness, decision-making, stress, automation, human-computer display, and interaction design principles. Students are expected to work individually or in a group on applying security functions to design a selected human factor-related project. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 765: *Quantum Information Processing and Security.* 3 credits.
This course explores advanced topics in quantum information processing and security, providing students with a deep understanding of quantum computing, communication, and information processing. It includes quantum algorithms, quantum cryptography, and the intersection of quantum computing with information security protocols. The course combines theoretical concepts with practical applications, preparing students to contribute to cutting-edge research in the field. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: Familiarity with basic concepts of information theory

Registration Restrictions:
Required Prerequisites: MATH 203[B-], 351[B-] and CS 367[B-].
[B-] Requires minimum grade of B-.

Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 770: *Fundamentals of Operating Systems.* 3 credits.
This project-oriented course delves into advanced principles and security problems governing the design and implementation of modern Operating Systems. Topics include advanced topics and open issues in virtual memory, kernel and user mode, system calls, threads, context switches, interrupts, interprocess communication, concurrency, processes and multi-threading, context switching, synchronization, scheduling, deadlock, memory management, dynamic memory allocation, and address translation. This course is offered to doctoral-level students who will master advanced OS concepts and security problems through a semester-long research project. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 780: *Advanced Hardware and Cyber-Physical Systems Security.* 3 credits.
Previously relegated to more complex systems of systems, the seamless integration of hardware and software components to efficiently reach design goals is now ubiquitous to a wide spectrum of systems.However, awareness and understanding of the security implications of such integration are not advancing at the same pace of its adoption, including in critical applications. This course explores the factors leading to such knowledge gap by providing an initial overview of the life-cycle of cyber-physical systems (CPS) with an emphasis on the associated security implications. Topics covered include best practices and policies for secure CPS design, the role of standardization, embedded threat detection and analysis, resiliency, CPS modeling and simulation, vulnerability and risk-assessment of CPS, and others. CPS security research is also emphasized, with students being exposed to the latest advances in CPS security, being expected to carry on CPS-security projects and/or research. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 785: *Advanced Unmanned Aerial Systems Security.* 3 credits.
This course provides engineers with an investigation on advanced topics and recent developments in the main technologies and operation aspects of Unmanned Aerial Systems (UAS), focusing on the associated counter measures and protective measures. It explores cutting-edge techniques for the safe and secure operation of UAS, especially in the context of contested environments. Topics are focused on UAS components, characteristics, and operational environment, such as weather and radio propagation. The course also covers active and passive detection of UAS, methods to avoid detection and for disrupting UAS operations, such as electromagnetic interfer-ence and cyberattacks, as well as measures against these methods, such as RADAR and IR stealth concepts. Finally, this course brings a holistic view of UAS security and

its future trends. The target audience consists of engineers interested in planning, de-signing, or participating in UAS operations from a safety and security standpoint. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 787: *Cyber Security Systems Engineering.* 3 credits.
This course addresses cyber security from the standpoint of systems engineers. It introduces core principles for the design and management of resilient and robust systems throughout their complete lifecycle. Topics include but are not limited to lifecycle assurance of systems, risk analysis, models for secure systems development and management, gap analysis, quantitative methods for cyber security, and special topics in cyber security. The course also covers distinct technologies for assessing system vulnerabilities, measuring and modeling risk, reducing uncertainty in risk management, and others. Target audience consists of engineers who want to expand their skill sets to better align with the demands of current cyber security jobs, as well as those who intent to work on cyber security research. Cyber security professionals would also benefit from the course by being exposed to a systems engineering, holistic perspective on cyber security design, development, and management. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit. Equivalent to CYSE 587, SYST 687, SYST 787.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus, Non-Degree or Senior Plus.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 789: *Advanced Artificial Intelligence Methods for Cybersecurity.* 3 credits.
This course explores the application of advanced concepts in artificial intelligence to cybersecurity. The focus is on the research and development of approaches for pre-dicting, detecting, and responding to cyber threats using technologies such as Bayesi-an networks, multi-entity Bayesian networks, search-based methods, decision mak-ing, causal learning, reinforcement learning, and others that can be applied to the se-curity of cyber physical systems. Current state-of-the-art AI-Based techniques will be discussed and potentially implemented in class. Students are expected to be familiar basic concepts in probability and statistics, discrete mathematics, decision-support systems, and optimization algorithms. Programming and software development skills in languages such as Python and Java are expected, although not at an advanced level. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May not be repeated for credit.
Recommended Prerequisite: CYSE 587, CYSE 689

Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 799: *Cyber Security Engineering Master Thesis.* 1-6 credits.
Research project chosen and completed under the guidance of a graduate faculty member, which results in a technical report acceptable to a three#member faculty committee, and an oral defense. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the degree.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy, Graduate or Non-Degree.

Students in a Non-Degree Undergraduate degree may **not** enroll.

Schedule Type: Thesis

Grading:
This course is graded on the Satisfactory/No Credit scale. (http://catalog.gmu.edu/policies/academic/grading/)

900 Level Courses

CYSE 998: *Doctoral Dissertation Proposal.* 3 credits.
Work on research proposal that forms basis for doctoral dissertation. Notes: No more than 24 credits of CYSE 998 and 999 may be applied to doctoral degree requirements. Offered by Cyber Security Engineering. May be repeated within the degree. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/engineering/cyber-security-engineering/). May be repeated within the degree.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy.

Enrollment limited to students in the Engineering Computing college.

Schedule Type: Dissertation

Grading:
This course is graded on the Satisfactory/No Credit scale. (http://catalog.gmu.edu/policies/academic/grading/)

CYSE 999: *Doctoral Dissertation.* 1-12 credits.
Formal record of commitment to doctoral dissertation research under direction of CYSE faculty member. Notes: Students must complete minimum 12 credits of doctoral proposal (CYSE 998) and doctoral dissertation research (CYSE 999) Maximum of 24 credits of CYSE 998 and 999 may be applied to degree. Students who choose to take less than 24 credits of CYSE 998 and 999 may earn remaining credits from approved course work. Students cannot enroll in CYSE 999 Advancement to Candidacy. Offered by Cyber Security Engineering (http://catalog.gmu.edu/colleges-schools/engineering-computing/

engineering/cyber-security-engineering/). May be repeated within the degree.
Registration Restrictions:
Enrollment limited to students with a class of Advanced to Candidacy.

Enrollment limited to students in the Engineering Computing college.

Schedule Type: Dissertation

Grading:
This course is graded on the Satisfactory/No Credit scale. (http://catalog.gmu.edu/policies/academic/grading/)