Graduate Certificate
Safety and Security of Autonomous Cyber-Physical Systems

Proposal 26-19
(Voting Units: Academic)

1. Proposal Date: 13 November 2018 - Revised 22 January 2019

2. Proposer Contacts and Departments:

William Predebon (wwpredeb@mtu.edu), Chair, Mechanical Engineering-Engineering Mechanics

Daniel Fuhrmann (fuhrmann@mtu.edu), Chair, Electrical and Computer Engineering

Steven Goldsmith (sygoldsm@mtu.edu), Research Professor and Instructor, Mechanical Engineering-Engineering Mechanics, Electrical and Computer Engineering

3. Sponsor Department Approvals: Attached at end of document

4. General Description and Characteristics of Program

The Departments of Mechanical Engineering-Engineering Mechanics and Electrical and Computer Engineering propose the establishment of the interdisciplinary *Graduate Certificate in Safety and Security of Autonomous Cyber-Physical Systems.* Students completing this certificate will demonstrate competencies in the hierarchical design, control, and integration of technologies into cyber-physical components and systems including modern networked and autonomous mobile systems for land, air, and water. While the certificate focus includes autonomous vehicles, the knowledge can be applied to other cyber-physical systems such as robots, manufacturing, and infrastructure. The competencies include threat analysis and vulnerability assessment, risk analysis for cyber-safety issues, systems engineering for safety and security, redundancy, fault-tolerance for modern mobility platforms, and the design and analysis of novel strategies for meeting emerging vehicle and other cyber-physical safety and security threats.

The certificate will be available to degree-seeking students enrolled in the Graduate School at Michigan Technological University, as well as non-degree seeking students employed in industry and at federal facilities and laboratories. Students enrolling in this certificate program must have an undergraduate degree in Mechanical Engineering, Electrical Engineering, or in a closely-related field that is primarily based on physical engineered systems. The certificate will be offered to on-campus students and online students. This certificate requires a minimum total of 15 credits.

Students must earn a grade of B or higher in each of the courses counting toward the certificate. A maximum of 6 credits is allowed in courses at the 4000-level.

The Director of Graduate Studies in each of the ME-EM and ECE departments will oversee the certificate program and acceptance for students in their departments, or most closely aligned with their departments.

Catalog Description -The Graduate Certificate in Safety and Security of Autonomous Cyber-Physical Systems provides knowledge of cyber-physical safety and security strategies arising from modern, advanced system control networks and interconnected system complexes.

Students accepted into this certificate program should have a *working understanding of mobile system components, control systems design and modeling, and computer networking.*

5. Rationale

In January 2016, Forbes magazine reported that more than 209,000 cybersecurity jobs were unfilled in the US alone. The shortfall of qualified cybersecurity engineers in the automotive area alone is further exacerbated by the need for deep knowledge of the embedded control and communications components of physical systems (including acceleration, braking, steering, stability, speed control, collision avoidance) that are physically integrated with the computers, software, sensors, and actuators that make up an autonomous system. Based upon discussions with a GM cybersecurity manager, other recent industry partners' input on new and emerging technologies in the automotive industry, and associated new job functions and hiring requirements, it is critical that students and incumbent engineers develop high-level skills targeted to meet the growing need for engineers to incorporate cyber-safety and security into the design of advanced components, controls, and communications among subsystems of autonomous cyber-physical systems of all types.

This certificate will also address safety and security of autonomous mobile platforms beyond automotive. Various recent press releases state:

- *Michigan Tech has a 64-year history of R&D in unstructured environments with the Tank Automotive Research, Development and Engineering Center (TARDEC) in Warren, MI coupled with years of testing and development at the Keweenaw Research Center. TARDEC conducts R&D in a number of laboratories including: Crew Station Systems Integration Laboratory, Robotic Systems Integration Laboratory, Ground Vehicle Simulation Laboratory, High Performance Computing Laboratory, Next Generation Software Laboratory, Center for Ground Vehicle Development and Integration, and the Ground Vehicle Power and Systems Engineering Laboratory.*

- *Michigan Technological University received $2.8 million from the US Department of Energy (DOE) to develop next-generation control systems for light-duty hybrid electric vehicles. Michigan Tech is one of three Michigan recipients of a total of $8.5 million in new grants from DOE’s Advanced Research Projects Agency-Energy (ARPA-E). One project, titled “Connected and Automated Control for Vehicle Dynamics and Powertrain Operation on a Light-Duty Multi-Mode Plug-in Hybrid Electric Vehicle”, will integrate advanced controls with connected and automated vehicle functions, enabling eco-routing and vehicle cooperative driving.*

- *The American Center for Mobility’s self-driving research site in Ypsilanti, Michigan, has established a new partnership with 15 Michigan universities, including Michigan Tech. The partnership will lead to training, courses, recruitment, internships, co-ops and work-study programs. The article was featured in* First Bell*, a daily science and engineering newsletter published by the American Society for Engineering Education (ASEE). In addition, Michigan Tech is one of three Michigan universities whose students have been invited to participate in a three-year autonomous vehicle competition sponsored by General Motors and the Society of Automotive Engineers (SAE).*

- *Michigan Technological University's Great Lakes Research Center was the site for the unveiling of the Marine Autonomy Research Site (MARS)–the first freshwater testbed of its kind in the world. Among the coalition's partner organizations is the Great Lakes-St. Lawrence Governors and Premieres, chaired by Governor Rick Snyder. The group's Executive Director David Naftzger said, "Shipping will look different in 25 years. Largely because of the work done here."*

- *Michigan Tech is in discussions to become a partner of the Institute on Public Policy and Law in Autonomy at Syracuse University.*

Michigan Tech has received encouragement from automotive industry OEMs, such as General Motors and Ford, for this curriculum development and for the past creation of several new courses in this area. Michigan Tech should offer recognition to students who complete a set of focused courses to give them a credential indicating their knowledge in this rapidly emerging field. Of special importance is the need to provide engineers and practitioners with coursework that emphasizes cyber-physical safety and security as a systems-engineering function, without the need for a traditional computer science background required by traditional cybersecurity courses. The cyber-physical courses account for background material that is suitable for mechanical and electrical engineers with automotive and other backgrounds. The focus of this certificate is on the physical hardware, the embedded controllers within that hardware, and the systems integration and communications among the subsystems to help ensure safety and security of massive and energetic systems operating autonomously including cars, trucks, military vehicles, ships, robots, manufacturing systems, and infrastructure.

This program will complement the existing *Graduate Certificate in Automotive Systems and Controls,* but this new program will focus on cyber-safety and security aspects and their impact on autonomous vehicles and other systems. This graduate certificate is already in demand: discussions with Army TARDEC, the above-mentioned OEMs, Michigan Automotive Defense and Cyber Awareness Team (MADCAT), and Tier 1 organizations (including Delphi, FEV, and Continental) have been positive and encouraging. Indeed, one Tier 1 manager of an autonomous driving unit has enrolled for courses in anticipation of this certificate becoming realized.

The *Graduate Certificate in Safety and Security of Autonomous Cyber-Physical Systems* will enable students to:

1) Apply modern cyber-safety and security analysis engineering principles to autonomous vehicles and a variety of systems involving onboard control networks, advanced automation, and collaborative vehicle and machine collectives;

2) Improve interdisciplinary skills in the analysis of complex systems with safety and security requirements; and

3) Communicate clearly with peers and management on established and emerging cyber-safety and security issues.

Students who complete this certificate will be able to demonstrate that they understand the cyber-safety and security issues for vehicles and interconnected systems, can apply that understanding to analyze and synthesize safe and secure cyber-physical systems, and effectively work at the intersection of cybersecurity and safety of autonomous systems.

6. Related Programs:

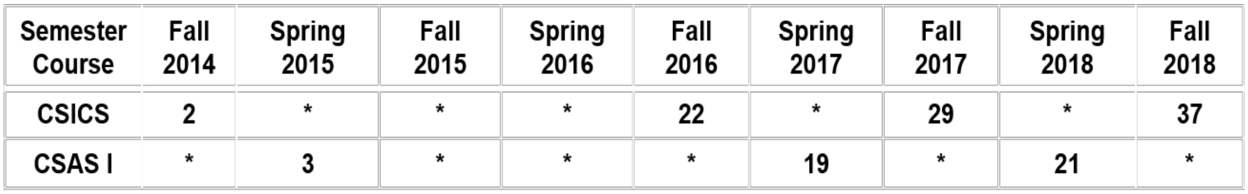
There are currently NO courses devoted to automotive cybersecurity and safety at any institutions of higher learning at this writing. Training in the form of 1-3 day industrial courses is available through the Society of Automotive Engineers, Vector Consulting Services, MIRA (Horiba MIRA – Kyoto, Japan), and a few other automotive suppliers. There are a variety of short courses held at various automotive cybersecurity conferences and summits covering general and special topics, such as the SANS Institute Automotive Cybersecurity Summit held in May, 2018. However, on

July 29, 2018 Gov. Rick Snyder announced a new program for Michigan high schools. “Masters of Mobility: Cyber Security on the Road” will provide in-depth training for Michigan high school teachers as well as resources and materials that will teach students to program, hack and learn to defend against cyber-attacks.

The proposed certificate has a strong focus on the intersection of cybersecurity with components, safety, vehicle and system controls, advanced operator assistance systems, vehicle and system communications (V2X), and autonomous operation to meet emerging industry needs. The certificate is aligned with the established *Graduate Certificate in Automotive Systems and Controls*, but is unique with respect to its focus on safety threats introduced by the cybersecurity issues of advanced automation, operator functions, and the interconnection of autonomous vehicles and systems for land, air, and water as well as in other applications in robotics, manufacturing, and infrastructure. The proposed certificate curriculum is also aligned with the new Master of Science in Cybersecurity offered by the Computer Science Department, but the proposed certificate is accessible to students in engineering, without a traditional CS background that does not address the dynamics and control of engineered physical systems.

7. Projected Enrollments:

Based upon historical enrollment of the two core courses shown in Table 1, and the expanded electives for this proposed certificate, it is estimated that the steady state student enrollment for the certificate will be 15-20 students.



Semester Course	Fall 2014	Spring 2015	Fall 2015	Spring 2016	Fall 2016	Spring 2017	Fall 2017	Spring 2018	Fall 2018
CSICS	2	*	*	*	22	*	29	*	37
CSAS I	*	3	*	*	*	19	*	21	*

Table 1. Historical enrollments for the certificate core courses CSICS = MEEM 5300/EE 5455 Cybersecurity of Industrial Control Systems, CSAS I = MEEM 5310/EE 5310 Cybersecurity of Automotive Systems I.

8. Scheduling Plans:

No change in the regular scheduling of the existing courses is anticipated. The Departments delivering the courses have agreed to fit them into their regular scheduling plans. All of the courses are now regularly offered.

9. Curriculum Design:

In accordance with Senate policy, the requirements for the *Graduate Certificate in Safety and Security of Autonomous Cyber-Physical Systems* are a minimum 15 credits of coursework, including the required minimum 9 credits of core and primary focus courses and up to 6 credits of approved electives. A grade of B or higher is required in all applicable courses and there is a maximum of 6 credits at 4000-level. Credits below 4000-level are not permissible toward the Certificate.

Required Coursework (Core) 6 credits – both of the following:

MEEM 5300 / EE 5455 Cybersecurity of Industrial Controls (3)

MEEM / EE 5315 Cybersecurity of Automotive Systems I (3)

Required Coursework (Primary Focus) 3 or more credits from the following:

EE 5365 In-Vehicle Communications Networks (3)

EE 5367 Vehicular Communications Networks (3)

MEEM / EE 5750 Distributed Embedded Control Systems (3)

MEEM / EE 5811 Automotive Systems (3)

EE / MEEM 5812 Automotive Control Systems (3)

MEEM / ECE 6320 Cybersecurity of Automotive Systems II (3)

Elective Coursework – up to 6 credits from the following:

CS 4471 / CS 5471 Computer Security (3)

MEEM 4730 Dynamic Systems Simulation (3)

MEEM 5430 Human Factors – Transportation (3)

CS 5472 Advanced Topics in Computer Security (3)

EE / CS 5821 Computational Intelligence (3)

EE / CS 5841 Machine Learning (3)

10. Course Descriptions: No new courses, all are currently offered.

Core and Primary Focus

MEEM 5300 / EE 5455 Cybersecurity of Industrial Controls (3) on campus & online
Steven Goldsmith (ME-EM/ECE)

General introduction to cybersecurity of industrial control systems and critical infrastructures. Topics include NIST and DHS publications, threat analysis, vulnerability analysis, red teaming, intrusion detection systems, industrial networks, industrial malware, and selected case studies.

MEEM / EE 5315 Cybersecurity of Automotive Systems I (3) on campus & online
Steven Goldsmith (ME-EM/ECE)

This course provides an understanding of modern automotive control and communications systems from a cyber safety and security perspective. Topics include: V2X communications, vehicle attack surfaces and vulnerabilities, in-vehicle networks, threat analysis and vulnerabilities, security mechanisms and architectures, security requirements analysis, hardware security modules, and standards (SAE J3061, Auto-ISAC, NHTSA).

EE5365 In-vehicle Communications Network (3) on campus
Aurenice Oliveira (ECE)

Course focuses on in-vehicle system domains and their requirements, and in-vehicle communication bus Controller Area Network (CAN) and its related physical layers standards. It also covers other buses such as LIN, FlexRay, MOST, Ethernet, as well as introduction to V2V and V21.

EE 5367 Vehicular Networking (3) on campus
Aurenice Oliveira (ECE)

Theories/principles, technologies, standards and applications of vehicular ad-hoc networks (VANET), as well as design considerations and main challenges to implement inter-vehicular communication networks. Topics include vehicle mobility modeling, physical layer considerations, routing protocols, and data security. Requires Linux OS, Python or C++.

MEEM / EE 5750 Distributed Embedded Control Systems (3) on campus
Bo Chen (ME-EM/ECE)

This course introduces embedded control system design using a model-based approach. Course topics include model-based embedded control system design, discrete-event control, sensors, actuators, electronic control unit, digital controller design, and communication protocols. Prior knowledge of hybrid electric vehicles is highly recommended.

MEEM / EE 5811 Automotive Systems (3) on campus & online
Jeff Naber (ME-EM)

Automotive systems for light duty vehicles are examined from the perspectives of requirements, design, technical, and economic analysis for advanced mobility needs. This course links the content for the automotive systems graduate certificate in controls, powertrain, vehicle dynamics, connected and autonomous vehicles.

EE / MEEM 5812 Automotive Control Systems (3) on campus & online
Jeff Burl (ECE)

Introduction to automotive control systems. Modeling and control methods are presented for: air-fuel ratio, transient fuel, spark timing, idle speed, transmission, cruise speed, anti-lock brakes, traction, active suspension systems, and hybrid electric vehicles, Advanced control methodologies are introduced for appropriate applications.

MEEM / EE 6320 Cybersecurity of Automotive Systems II (3) on campus & online
Steven Goldsmith (ME-EM/ECE)

This course covers advanced topics in cybersecurity of automotive systems. Some topics include communications security for V2X systems, vulnerabilities in cooperative vehicle infrastructures (CVI) such as intersection collision avoidance systems and platooning, threat analysis for CVI, and security issues introduced by autonomous driving systems operating at SAE J3016 Autonomy Levels 3, 4 and 5.

Electives

CS 4471 / CS 5471 Computer Security (3) on campus
Bo Chen (CS)

Development and administration of secure software systems. Topics include principles of software development, practical cryptography, program security, operating system security, database security and administration, legal and ethical issues.

ECE 4723 Network Security (3) on campus
Christopher (Kit) Cischke (ECE)

Learn fundamentals of cryptography and its applications to network security. Understand network security threats, security services, and countermeasures. Acquire background knowledge on well-known network security protocols. Address open research issues in network security.

MEEM 4730 Dynamic System Simulation (3) on campus & online
Gordon Parker (ME-EM)

Methods for simulating dynamic systems described by ordinary differential equations using numerical integration are developed. Quantifying simulation errors for both batch and real-time, control system applications is covered along with numerical optimization strategies for model validation. MATLAB and Simulink are used to illustrate key concepts.

MEEM 5430 Human Factors-Transportation (3) on campus & online
Ye Sun (ME-EM)

This course aims to provide an understanding of drivers as a system component in the operation of vehicles and other transportation systems. Topics covered include human factors, driver-vehicle interaction, intelligent transportation systems, connected vehicle technology, and user interface.

CS 5472 - Advanced Topics in Computer Security (3) on campus
Bo Chen (CS)

This course covers various aspects of producing trusted computer information systems. Topics include network perimeter protection, host-level protection, authentication technologies, formal analysis techniques, and intrusion detection. Current systems will be examined and critiqued.

EE / CS 5821 - Computational Intelligence-Theory and Application (3) on campus
Timothy Havens (ECE/CS)

This course covers the four main paradigms of Computational Intelligence, viz., fuzzy systems, artificial neural networks, evolutionary computing, and swarm intelligence, and their integration to develop hybrid systems. Applications of Computational Intelligence include classification, regression, clustering, controls, robotics, etc.

EE / CS 5841 - Machine Learning (3) on campus
Anthony Pinar (ECE)

This course will explore the foundational techniques of machine learning. Topics are pulled from the areas of unsupervised and supervised learning. Specific methods covered include naive Bayes, decision trees, support vector machine (SVMs), ensemble, and clustering methods.

11. Model Schedule Demonstrating Completion Time:

It is anticipated that degree-seeking students will take at a minimum one course each semester toward the certificate, since certificate credits can be counted toward a degree. It is expected that students will take additional courses each semester so that the certificate is completed within 3-4 semesters. It is also anticipated that the majority of non-degree seeking students will be online students who will take one course each semester toward the certificate, hence it is expected that these students will complete the certificate in five semesters. The core and primary focus courses are offered on the following schedule. Elective courses are regularly taught on campus and will be placed online based on demand. Two elective courses must be completed in addition to the Core and Primary Focus courses.

Core (both required)

MEEM 5300 / EE 5455	Cybersecurity of Industrial Control Systems	Fall
MEEM 5315 / EE 5315	Cybersecurity of Automotive Systems I	Spring

Primary Focus (one required)

EE 5365	In-Vehicle Communications Networks	Fall
MEEM 5811 / EE 5811	Automotive Systems	Fall
MEEM 6320 / EE 6320	Cybersecurity of Automotive Systems II	Fall
EE 5367	Vehicular Communications Networks	Spring
MEEM 5750 / EE 5750	Distributed Embedded Control Systems	Spring
EE 5812 / MEEM 5812	Automotive Control Systems	Spring

12. Library and other Learning Resources: Students in this program will need only the Library resources presently available to all enrolled students.

13. Faculty Resumes:

Jeffrey Burl (ECE)	http://www.mtu.edu/ece/department/faculty/full-time/burl/
Bo Chen (CS)	http://www.mtu.edu/cs/department/faculty-staff/faculty/chen/
Bo Chen (ME-EM/ECE)	http://www.mtu.edu/mechanical/people/faculty/chen/
Christopher (Kit) Cischke (ECE)	http://www.mtu.edu/ece/department/faculty/full-time/cischke/
Steven Goldsmith (MEEM/ECE)	https://www.mtu.edu/mechanical/people/scholars-instructors/goldsmith/
Timothy Havens (ECE/CS)	http://www.mtu.edu/ece/department/faculty/full-time/havens/
Jeff Naber (ME-EM)	http://www.mtu.edu/mechanical/people/faculty/naber/
Aurenice Oliveira (ECE)	http://www.mtu.edu/ece/department/faculty/full-time/oliveira/
Gordon Parker (ME-EM)	http://www.mtu.edu/mechanical/people/faculty/parker/

Anthony Pinar (ECE)	http://www.mtu.edu/ece/department/faculty/full-time/pinar/
Ye Sun (ME-EM)	http://www.mtu.edu/mechanical/people/faculty/sun/

14. Equipment: No additional equipment will be required.

15. Program Costs: The courses are presently being taught on a regular basis and are expected to cover the demand. Resources, such as on-line software, are already provided and available to instructors.

16. Space: No additional space is required.

17. Policies, Regulations, and Rules: Credits earned for this certificate may also be applied toward a single graduate degree at Michigan Technological University per Senate Policy 411.1

18. Accreditation Requirements: Michigan Tech is accredited by the Higher Learning Commission (HLC) (https://www.mtu.edu/provost/accreditation/hlcommission/). The proposed certificate will not require additional accreditation. The proposed certificate will meet HLC criteria 3 and 4.

19. Planned Implementation Date: Fall 2019

20. Assessment:

Students will demonstrate proficiency in the subject matter through the successful completion of the required and elective coursework. A portion of the students will be degree-seeking, while others will be non-degree seeking pursuing only the certificate.

The Graduate Student Learning Objective for this certificate is:

- Demonstrate an understanding of cyber-safety and security issues for vehicles and interconnected systems,
- Apply that understanding to analyze and synthesize safe and secure cyber-physical systems, and
- Effectively work at the intersection of cybersecurity and safety of autonomous systems.

The assessment points for this objective will be grades earned in the 15 credits of coursework for the certificate. The two core courses of the certificate contain required written reports further demonstrating proficiency of the subject matter. The written reports will be assessed and reported using a separate metric from the course grades. The Graduate Director of the department of the undergraduate degree or admission (ME-EM or ECE) will compile the assessment points at the time the certificate audit or degree schedule is completed, and make it part of their graduate assessment portfolio.

For those students completing the certificate as non-degree seeking, the same procedure will be followed at the time the certificate audit is approved, with the certificate assessment as a separate section of the department's assessment reporting.