Automotive Cybersecurity (Certificate)

Catalog Effective Term:
Program Code: CTACYB
Credential: Certificate
High Demand Occupation, High Skill Occupation, High Wage Occupation

This certificate program is designed to meet the emerging demand for highly skilled automotive cybersecurity professionals. In this certificate program, students are introduced to the skills and strategies needed to test security related to automobile networks and related infrastructure. Students will work with the various automobile networks (CAN, LIN, Ethernet, and FlexRay) and explore protocols and messages produced by the vehicle that could be vulnerable to attacks. Students will consider risk mitigation technologies including authentication, encryption and firewall technologies.

Learners in this program acquire the following skills:

- Learn basic networking concepts including V2V, V2I and V2X communication
- Understand common security terms and concepts and how they relate to automobiles in both a technical and compliance nature
- Understand relevant vehicle technologies including ECU's (Electronic control unit) and basic electrical theory
- Read and write basic computer programs and scripts
- Develop process and procedures for testing the security of a vehicle's information network
- Practice reverse engineering techniques for testing security

Minimum Credits Required for the Program: 19

Major/Area Requirements

ATT 131	Automotive Electrical	4
CPS 120	Introduction to Computer Science	3
CST 185	Local and Mobile Networking Essentials	4
CSS 200	Introduction to Network Security - Security+	4
CSS 285	Essentials of Automotive Penetration Testing	4
Total Credits		**19**

Program Information Report

Science, Computer Technology, Engineering & Math

Automotive Cybersecurity (CTACYB)

Certificate

Program Effective Term: Fall 2020

High Demand Occupation High Skill Occupation High Wage Occupation

This certificate programs is designed to meet the emerging demand for highly skilled automotive cybersecurity professionals. In this certificate program, students are introduced to the skills and strategies needed to test security related to automobile networks and related infrastructure. Students will work with the various automobile networks (CAN, LIN, Ethernet, and FlexRay) and explore protocols and messages produced by the vehicle that could be vulnerable to attacks. Students will consider risk mitigation technologies including authentication, encryption and firewall technologies.

Learners in this program acquire the following skills: Learn basic networking concepts including V2V, V2I and V2X communication; Understand common security terms and concepts and how they relate to automobiles in both a technical and compliance nature; Understand relevant vehicle technologies including ECU's (Electronic control unit) and basic electrical theory; Read and write basic computer programs and scripts; Develop process and procedures for testing the security of a vehicle's information network; Practice reverse engineering techniques for testing security.

Major/Area Requirements		(19 credits)
ASV 131	Automotive Electrical	4
CPS 120	Introduction to Computer Science	3
CSS 200	Introduction to Network Security - Security+	4
CSS 285	Essentials of Automotive Penetration Testing	4
CST 185	Local and Mobile Networking Essentials	4

Minimum Credits Required for the Program: 19

Received C&A 2/6/20

Washtenaw Community College

PROGRAM PROPOSAL FORM

☒ **Preliminary Approval –** Check here when using this form for preliminary approval of a program proposal, and respond to the items in general terms.

□ **Final Approval** – Check here when completing this form after the Vice President for Instruction has given preliminary approval to a program proposal. For final approval, complete information must be provided for each item.

Program Name:	Automotive Cybersecurity	**Program Code:**
Division and Department:	BCT - CSIT	CTACYB
Type of Award:	□ AA □ AS □ AAS ☒ Cert. □ Adv. Cert. □ Post-Assoc. Cert. □ Cert. of Comp.	
Effective Term/Year:	Fall 2020	**CIP Code:**
Initiator:	Cyndi Millns	11.1003
Program Features Program's purpose and its goals. Criteria for entry into the program, along with projected enrollment figures. Connection to other WCC programs, as well as accrediting agencies or professional organizations. Special features of the program.	The purpose of the Automotive Cybersecurity certificate program is to educate and train a future workforce in connected vehicle technologies and related threats in order to create a more secure mode of transportation. The program will combine courses in the Computer Science and Information Technology department with courses in the Automotive Service Technology department in the first level certificate with implementation of additional infrastructure based technologies in an advanced certificate (to include programmable logic controllers and technology related to a vehicle to infrastructure environment) – forthcoming. The program will be a part of the Advanced Transportation Center. Students who complete this program will gain an understanding of automotive network systems and related threats. Automotive attack surfaces will be highlighted, with a focus on attack techniques to provide insight into creating secure automotive systems. Students will complete hands-on exercises including reverse engineering in a lab environment that will highlight offensive methodologies with a follow up on defensive strategies. The Mobile Hacking workbench that was purchased in Fall 2018 will be used for reverse engineering the CAN bus of the vehicle (2012 Ford Focus) and additional test benches and connected vehicle will be obtained/purchased for testing and securing more recent technologies. This equipment will be purchased for use in the new Automotive Cybersecurity Lab that will be built as part of the Advanced Transportation Center and will allow for scalability in a multi-student lab based environment. Students will be prepared and encouraged to participate in the Society of Automotive Engineer's Cyber Auto Challenge that takes place every summer based on an application and entry assessments and provides an opportunity to extend learning capacity in automotive cybersecurity as well as connect students and employers in a hands-on environment.	

Need Need for the program with evidence to support the stated need.	Today there are over 100 million lines of code in the average modern high end vehicle with multiple entry points for bad actors. As the threat of nation state hackers is on the rise, securing our critical infrastructure in the area of mobility has never been more important. Automotive companies have expanded their hiring needs to include Automotive Cyber Security Technicians and Engineers. These individuals will not only understand cyber security but be able to think like a hacker in order to make vehicles and the connected infrastructure safe from attacks.

Program Outcomes/Assessment State the knowledge to be gained, skills to be learned, and attitudes to be developed by students in the program. Include assessment methods that will be used to determine the effectiveness of the program.	Outcomes The proposed Pen Testing Automotive Platforms course will be the Capstone course in this program and will assess the following outcomes: 1. Identify and use processes and procedures for testing the security of a vehicle's information network. 2. Explain the components and protocols surrounding vehicle security. 3. Test the security of a vehicle network in order to find vulnerabilities. 4. Apply regulatory and compliance standards to connected vehicles.	Assessment method 1. Outcome-related questions on the departmentally-developed objective final exam. 2. Departmentally-developed skills exam

Curriculum List the courses in the program as they should appear in the catalog. List minimum credits required. Include any notes that should appear below the course list. Associate degree programs must provide a semester by semester program layout.	**CST 185: Local and Mobile Networking Essentials (4 credit hours)** Students learn basic networking concepts including building networks, connecting to a network and connecting networks. Included are peer-to-peer, client/server relationships, network topologies, media, architectures, the OSI model, Ethernet and TCP/IP protocols, IPv4/IPv6 and MAC addressing, routers/routing, network printing, NAT, VPN's, wireless, serial communication, Bluetooth, NFC, and DSRC. The course also provides a strong foundation in preparation for the CompTIA Network+ Exam. **CSS 200: Introduction to Network Security – Security+ (4 credit hours)** In this course, students learn the fundamentals of network security. Topics to be covered include understanding security measures, techniques for securing systems, legal issues, basic intrusion detection and recovery methods. Many of the topics required for the Security+ certification will be covered. This course helps students prepare for the CompTIA Security+ Certification. The student is expected to have a basic knowledge of Linux, Windows, working at the command line of any Operating System and networking. **ASV 131: Automotive Electrical (4 credit hours)** In this course, students will learn basic electrical theory, use and interpretation of automotive wiring diagrams, and use of electrical testing equipment. Students will learn the skills needed to diagnose and replace a number of commonly serviced electrical components. The focus of this course allows students to gain practical experience in the laboratory. **CPS 120: Introduction to Computer Science (3 credit hours)** This course is an introduction to computer science for those planning to take advanced courses in the computer programming field or for those who do not want to take

programming courses but a computer course is required. Students learn to write, enter, compile and execute simple computer programs. This course is intended to bridge the gap between a basic computer literacy and advanced courses. Topics include numbering systems, operating systems, database, programming, networking, Internet and algorithms. Students must have basic computer literacy in order to be successful in this course.

CSS 285: Pen Testing Automotive Platforms (proposed 4 credit hours)
In this course, students will gain an understanding of the automotive cybersecurity threat-landscape. Automotive attack surfaces will be highlighted, with a focus on attack techniques to provide insight into creating secure automotive systems. Students will complete hands-on exercises including reverse engineering in a lab environment that will highlight offensive methodologies with a follow up on defensive strategies.

Budget

Specify program costs in the following areas, per academic year:

10 Test Benches with vehicle and instrumentation work.

	START-UP COSTS	ONGOING COSTS
Faculty	$.	$.
Training/Travel	.	.
Materials/Resources	.	.
Facilities/Equipment	182,550.00	.
Other	55,000.00	.
TOTALS:	$ 237,550.00	$.

Program Description for Catalog and Web site

In this certificate program, students are introduced to the skills needed to test security related to automobile networks and related infrastructure, including Vehicle–to–Vehicle (V2V), Vehicle–to–Infrastructure (V2I) and Vehicle–to–Everything (V2X) communications. Students will understand relevant vehicle technologies, protocols and messages produced by the vehicle that could be vulnerable to attacks. Students will consider risk mitigation technologies, including authentication, encryption and firewall technologies. This certificate program is designed to meet the emerging demand for highly skilled automotive cybersecurity professionals.

Program Information

Accreditation/Licensure – This could be a focus area within the Center of Academic Excellence Designation through the National Security Agency.

Advisors - Sandro Tuccinardi, Cyndi Millns

Advisory Committee – Subgroup of the Cybersecurity Advisory Committee (10 members)

Admission requirements -

Articulation agreements – Walsh (to be developed)

Continuing eligibility requirements -

Assessment plan:

Program outcomes to be assessed	Assessment tool	When assessment will take place	Courses/other populations	Number students to be assessed
1. Identify and use appropriate processes and procedures for testing the security of a vehicle's information network.	1. Outcome-related questions on the departmentally-developed objective final exam. 2. Departmentally developed skills exam (Lab)	Every three years	All sections	1. All students 2. Random sample of 50% of all students with a minimum of 1 full section
2. Explain the components and protocols surrounding vehicle security.	1. Outcome-related questions on the departmentally-developed objective final exam.	Every three years	All sections	All students
3. Test the security of a vehicle network in order to find vulnerabilities.	Departmentally developed skills exam (Lab)	Every three years	All sections	Random sample of 50% of all students with a minimum of 1 full section
4. Apply regulatory and compliance standards to connected vehicles.	1. Outcome-related questions on the departmentally-developed objective final exam.	Every three years	All sections	All students

Scoring and analysis plan:

1. Indicate how the above assessment(s) will be scored and evaluated (e.g. departmentally-developed rubric, external evaluation, other). Attach the rubric.
   Departmentally-developed rubric

2. Indicate the standard of success to be used for this assessment.
   70% of students assessed will score 70% or higher

3. Indicate who will score and analyze the data.
   Department Faculty

REVIEWER	PRINT NAME	SIGNATURE	DATE
Department Chair/Area Director	Cyndi Millns	Cyndi Millns	2-4-2020
Dean	Eva Samulski	E. Samulski	2-6-2020
Curriculum Committee Chair	Lisa Veasey	Lisa Veasey	3/3/2020
Please submit completed form to the Office of Curriculum and Assessment (SC 257). Once reviewed by the appropriate faculty committees, we will secure the signature of the VPI and President.			
Vice President for Instruction ☐ Approved for Development ☐ Final Approval	Kimberly Hurns		3/3/2020
President	Rose Bellanca	Rose B. Bellanca	5/20/20
Board Approval	▨	▨	4/28/20

Reviewed by C&A Committees
2/20/20