Annual Assessment Report for Academic Programs

The University Assessment Team advocates for the enhancement of student learning through purposeful, meaningful, and feasible student-outcomes assessment practices. The Assessment Team seeks to collaborate with programs, departments, and units to ensure that effective assessment of student learning occurs across the University. To assist in meeting this goal, the Team requests that you complete this Annual Assessment Report form to document student learning in your program. A PDF version of this completed form will be posted to the Academic Affairs Assessment website. Please note that this Annual Assessment Report form should only be completed after you have an Assessment Plan for Academic Programs forms on file with the University Assessment Team. The plan is completed once and only updated when revisions have been made to components of the plan.

1. Degree Level and Program Name: Master of Science in Vehicle Cyber Security

2. College/School: College of Engineering & Science

3. Assessment Overview - Briefly share how student learning outcomes assessment is conducted within your program/department (e.g. number of outcomes, examples of assignments used, and frequency of assessment).

The Master of Science in Vehicle Cyber Engineering program has five student learning outcomes. In year 1, we assess Learning Outcomes 1 and 2. In year 2, we evaluate Learning Outcomes 3 and 4, and in the third year, we focus on Learning Outcome 5.
This year's annual assessment cycle will be evaluating Learning Outcomes 3 and 4.

4. Student Learning Outcomes -Which student learning outcome(s) from the assessment plan filed with the University Assessment Team is/are being reported on in this report? Include the corresponding benchmark(s) for each outcome.

Based on the Master of Science in Vehicle Cyber Engineering's Program Assessment Plan on file with the University Assessment Team, two outcomes are being assessed in this cycle.

• Student Learning Outcome #3: Develop cybersecurity solutions for embedded vehicle systems and distributed in-vehicle networks. The benchmark for success is to have at least 70% of the students earn a rubric equivalent score of a C or better on the Quizzes, technical papers, and the Term project in VCE 5500 – Secure Vehicle Electronics.

• Student Learning Outcome #4: Identify, formulate, and solve cybersecurity problems in the areas of vehicular networks, artificial intelligence, and supply chain. The benchmark for success is to have at least 70% of the students earn a rubric equivalent score of a C or better on the homework, technical papers, and the Term project in VCE 5150 – Secure Wireless Vehicular Networks.

Institutional Outcomes - For which institutional outcome(s) do the reported student learning outcome(s) align?

SLO Outcome Alignment	Institutional Outcome
	I. Jesuit & Mercy Values
	II. Diversity & Cultural Awareness
Yes	III. Critical Thinking & Problem Solving
Yes	IV. Communication
	V. Professionalism
	VI. Lifelong Learning

6. **Assessment Period:** Select the academic year for which you are reporting results (i.e. when data were collected):

2023-2024

7. **Results, Planned Actions, and/or Actions Taken** -Briefly summarize the assessment results, how they relate to benchmark(s), and how you are using them to enhance student learning and improve program quality.

Student Learning Outcome #3: Develop cybersecurity solutions for embedded vehicle systems and distributed intra-vehicle networks.

Research Papers 1 and 2 are individual projects in which students submitted research papers covering the following topics:
- CAN and Ethernet vehicle technologies
- Autonomous vehicles and their security levels
- Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) security
- Risk analysis
- Security and quality of service

Students must understand computer network architecture, Ethernet communication protocols, basic electrical circuits, and cryptography. They also need to become familiar with cybersecurity hardware tools to effectively execute attacks on vehicles across various surfaces, using tools like Vehicle SPY and Wi-Fi Pineapple. Additionally, students are required to be familiar with programming languages such as C, C++, Python, or other relevant languages.

The assessment of students' quizzes, projects, and papers yielded marks ranging from 70% to 94%, indicating a generally high level of achievement.

Refer to the Table in the attached Annual Assessment Report for assignment grade details.

Student Learning Outcome #4: Identify, formulate, and solve cybersecurity problems in the areas of vehicular networks, artificial intelligence, and supply chain.

Research papers 1 and 2 are individual projects, and the students provided research papers covering the following topics:
- Wi-Fi, BT and NFC

- 5G Mobile Cellular Network and Security
- Risk analysis
- Design Failure Mode and Effect Analysis (DFMEA)

Students need to be aware of computer network architecture, Ethernet communication protocols, basic electrical circuits, and cryptography. They must also be familiar with cybersecurity hardware tools to effectively carry out attacks on vehicles across various surfaces, such as Vehicle SPY and Wi-Fi Pineapple. Additionally, students are required to have knowledge of programming languages such as C, C++, Python, or any other programming language.

The assessment of the students' homework, papers, and projects yielded a range of marks from 70% to 90%, indicating a generally high level of achievement.

Refer to the Table in the attached Annual Assessment Report for assignment grade details.

Attachment(s):

Annual Assessment report - VCE March 29 2025_ Paul Spadafora.docx