|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| **Reflection Report** |
| |  |  |  | | --- | --- | --- | | Milad Chowdhury | 6/7/25 | Secure Systems Architecture April 2025 | |

Contents

[Reflection on Collaborative Development of a Secure CPS Simulation Project 2](#_Toc200150246)

[WHAT? – Project Summary and My Role 2](#_Toc200150247)

[SO WHAT? – Reflection on Experience and Emotions 2](#_Toc200150248)

[NOW WHAT? – Lessons and Professional Application 2](#_Toc200150249)

[Professional Development and Learning Summary 3](#_Toc200150250)

[References 4](#_Toc200150251)

## Reflection on Collaborative Development of a Secure CPS Simulation Project

This reflection evaluates my contribution and personal learning while developing a simulated secure Cyber-Physical System (CPS). It applies the Rolfe et al. (2001) reflective framework to assess the team experience, technical implementation, and lessons applicable to future projects and professional development. This reflection meets the module's learning outcomes by critically analysing secure system implementation, collaboration, and testing under constrained conditions.

## WHAT? – Project Summary and My Role

This module required designing and implementing a secure, distributed CPS prototype using Python. Our team simulated six IoT clients interacting with a central controller, applying Fernet encryption and Quality of Service (QoS) simulation to test delivery reliability and security vulnerabilities. Although my hypothesis — that client-side encryption with QoS improves resilience — was not initially adopted, the team later recognised its relevance, giving me a key role in technical delivery and vulnerability mitigation. I led the architecture and implementation of client scripts, the QoS module, and CWE-based validation logic. I also created and maintained output datasets (\*results.csv\*) and runtime logs (\*log\_controller.txt\*), which helped the group provide measurable evidence for security risk evaluation, addressing learning outcomes on identifying and mitigating operating system vulnerabilities.

## SO WHAT? – Reflection on Experience and Emotions

Initially, I was apprehensive about team dynamics and aligning technical tasks with academic expectations. However, consistent communication through WhatsApp and clear role division reduced ambiguity. I received encouraging feedback from peers like Louis and James, especially regarding my modularisation of the sensor logic and consistency in CWE mapping. A key emotional learning moment came when initial tests failed due to inconsistent output logging. Tutor feedback in Units 4-6 highlighted the importance of traceability. I redesigned the CSV format to include timestamped records and CWE IDs, which clarified test results and directly supported the final report. Interpersonally, I became more aware of the ethical dimensions of collaboration, acknowledging peer input, maintaining transparency on progress, and ensuring shared credit. I also realised the importance of emotional regulation when balancing group deadlines with personal accountability.

## NOW WHAT? – Lessons and Professional Application

This module enhanced my technical and professional skills. I learned to convert threat modelling into testable code, apply CWE references, and simulate real-world vulnerabilities. Our logs and test cases align with OWASP Proactive Controls and NIST guidance, validating our approach. I plan to use Git for better team visibility, integrate unit tests and CI pipelines, and explore Docker for simulating multiple devices. This experience will aid my pursuit of software architecture roles in IoT or embedded systems, providing me with practical knowledge for real-world design applications.

## Professional Development and Learning Summary

I developed various technical and soft skills aligned with the module learning outcomes throughout this project. My time management improved significantly as I shifted from a reactive to a proactive approach using task trackers and setting short-term deadlines. My understanding of secure system design evolved from surface-level encryption to applied threat modelling using CWE references and OWASP standards. Regarding testing practice, I moved from inconsistent manual testing to implementing structured log output and test-driven evaluations. My collaboration skills were also strengthened, particularly in virtual settings, where I learned the value of clear task division, transparent feedback, and shared accountability. Moving forward, I intend to integrate more advanced tools such as Git for version control, automated CI pipelines for consistent testing, and containerisation tools like Docker for scalability. This reflective development process has prepared me for academic and professional roles involving secure software architecture.

**Word Count: 575 words**

## References

Rolfe, G., Freshwater, D., & Jasper, M. (2001). Critical reflection in nursing and the helping professions: a user’s guide. Palgrave Macmillan.  
NIST (2015). SP 800-82r2: Guide to Industrial Control Systems (ICS) Security. https://nvlpubs.nist.gov  
MITRE (2025). Common Weakness Enumeration (CWE). https://cwe.mitre.org  
Tutor Feedback (2025). Unit 4-6 discussion