ENGI 9839 – Software Verification & Validation

Project Proposal

Professor: Raja Manzar Abbas

Team Members:

1. Anil Manyam – 202483873
2. Sadia Alam – 202295835

Project Idea:

Title: Verification and Validation of a Design-by-Contract Layered Library Management System

Proposal:

In this project we aim to verify and validate the correctness and reliability of the Library Management System (LMS) which uses Design by Contract (DbC) principles within a layered architecture.

To ensure the LMS adheres to its specified behavior, we are planning to apply both formal methods and practical validation techniques focused on the following key aspects:

We are planning to use the following methods: (As of Now)

- Alloy Model Checking: Key functions such as borrowing books will be formally specified in Alloy to verify system properties like borrowing limits, book availability, and state consistency.

- Runtime Verification with PyContracts: DbC contracts (preconditions, postconditions) will be tested in Python using PyContracts to ensure correctness during execution.

- Unit Testing and Oracles: We will write automated tests using pytest and define expected outputs to act as test oracles for validating implementation correctness.

We think that this project may bridges formal verification and practical validation to assess the reliability of our LMS design.