**Project Assignment: Formal Methods in Software Engineering**

**Title: Applying Formal Methods for Software Verification**

**Objective**:  
The goal of this project is to give students hands-on experience in applying formal methods to ensure the correctness, reliability, and safety of software. Students will select a problem domain, model the system using a formal specification language, and verify the implementation using tools and frameworks discussed in class.

**Project Outline:**

**Problem Statement:**

Choose one of the following software domains and create a formal model of the system:

1. **Traffic Light Controller**  
   Model and verify a traffic light system to ensure proper transitions between light states (e.g., Red → Green → Yellow → Red).
2. **Banking System (Transaction Validation)**  
   Design a simple banking system that verifies transaction rules, such as ensuring no overdraft or double withdrawals.
3. **Access Control System**  
   Model an access control system to verify permissions and ensure no unauthorized access occurs.
4. **Sorting Algorithm**  
   Verify the correctness of a sorting algorithm (e.g., QuickSort or MergeSort) to ensure the output is always sorted.

**Tasks and Deliverables:**

1. **Formal Specification (Day 1-2)**
   * Choose one of the above systems or propose your own
   * Develop a formal specification of the system using a formal specification language like Z, Alloy, or VDM.
   * Clearly define the system's requirements, invariants, and constraints.
2. **Model Implementation (Day 3-5)**
   * Implement the system in a suitable programming language (e.g., C, Java, or Python).
   * Use formal verification tools (e.g., SPARK, Dafny, Frama-C) or frameworks (e.g., CBMC, KLEE) to verify the correctness of your implementation.
   * Verify properties such as:
     + Safety (e.g., no invalid states).
     + Functional correctness (e.g., system behaves as intended).
3. **Testing and Documentation (Day 6-7)**
   * Perform testing using automated or manual approaches to validate the results.
   * Write a short report (2-3 pages) summarizing:
     + Problem statement and requirements.
     + Formal specification and modeling process.
     + Verification results and any bugs/issues found.
     + Key challenges and lessons learned.

**Assessment Criteria:**

| **Component** | **Weightage** |
| --- | --- |
| **Formal Specification** | 30% |
| **Implementation and Verification** | 50% |
| **Documentation** | 20% |

**Resources:**

* **Tools**: Dafny, SPARK, Frama-C, KLEE, CBMC
* **References**:
  + [Alloy Analyzer](https://alloytools.org/)
  + SPARK User Guide
  + VDM Tutorials

**Submission Deadline**: 31/12/2024.

**Note**: Collaboration is allowed in pairs. Ensure proper version control and share your code repository (e.g., GitHub link) for evaluation.