COURSE SYLLABUS

Course Code:
Course Name: Formal Engineering Methods for Software Quality Assurance
Credits:
Total Hours:
Semester: Spring
Instructors: Shaoying Liu
Textbooks: Formal Engineering for Industrial Software Development, Springer-Verlag, 2004, ISBN 3-540-20602-7.

中文名：软件开发的形式化工程方法 – 结构化+面向对象+形式化，Shaoying Liu 著，清华大学出版社，2008（影印版）。

Prerequisites:

(1) Predicate logic and set theory (basics)
(2) Programming language (any language)

Description:

Conventional software engineering based on informal or semi-formal methods are facing tremendous challenges in ensuring software quality. Formal methods have attempted to address those challenges by introducing mathematical notation and calculus to support formal specification, refinement, and verification in software development. However, in spite of their theoretical potential in improving the controllability of software process and reliability, formal methods are difficult to apply to large-scale and complex systems in practice due to many constraints (e.g., limited expertise, complexity, changing requirements).

``Formal Engineering Methods'' (FEM) has been proposed and developed as a research area since 1997 to study how formal methods can be effectively integrated into conventional software engineering process to improve software productivity and quality in practice. A specific representative FEM called Structured Object-Oriented Formal Language (SOFL) has also be developed over the last two decades that offers three rigorous but practical techniques for system modeling and verification: three-step formal specification approach, specification-based inspection, and specification-based testing. The effective combination of these three techniques can significantly enhance software productivity and quality.

This course aims to teach students how formal engineering techniques can be effectively used in conventional software engineering process to enhance software productivity and quality through introducing SOFL. After learning this course, students are expected to understand (1) essential knowledge and skills for writing formal specifications, (2) how to construct formal specifications based on informal requirements, (3) how to balance simplicity, visualization, and precision in software development, and (7) future research directions in formal engineering methods.

Course Topics:

(1) Introduction to Formal Engineering Methods (FEM) (why FEM, what is FEM, and relations among formal methods, FEM, and software engineering)

(2) Introduction to a specific FEM: SOFL (Structured Object-Oriented Formal Language).

(3) The SOFL Specification Language

1. Modules
2. Condition Data Flow Diagram (CDFD)
3. Implicit process specification (pre-post notation)
4. Implicit and explicit function specifications
5. Basic types and operators
6. Set types and operators
7. Sequence types and operators
8. Composite types and operators
9. Product types and operators
10. Map types and operators
11. Union types and operators
12. Process decomposition and hierarchy of CDFDs

(4) a Three-Step Formal Specification Approach

(5) **Course Schedule:**

Weeks	**Contents**	**Categories**
		Lecture
		Discussion sections