

FORMAL METHODS ENGINEERING (SE-O-03)

AIMS:

Formal methods are those with a sound basis in mathematics. They are often used in the specification and design of critical systems where failure can cause catastrophic effects such as death, damage to the environment, lose of money, etc. However, the use of these methods in a large scale design and development still not wide spread as originally thought. What is needed is mechanisms to engineer these methods so that they can be used in industry and on large scale systems.

This module is intended to provide the student with a comprehensive understanding, critical evaluation of formal methods and gives a detail account on a particular technique that is based on automata theory and their industry-strength tool support such is Statemate.

LEARNING OUTCOMES:

Upon successful completion of this module, the student will be able to:

- critically evaluate the basis for the need of trustworthiness in large scale computer systems;
- critically evaluate fundamentals of formal methods;
- appreciate the essential issues of using formal techniques in the whole system life cycle in particular requirement engineering and architecture design;
- critically evaluate various types of large scale system from transformational to hybrid systems;
- critically evaluate the role of tools and methods for the engineering formal methods.

SYLLABUS CONTENT:

- Large scale systems.
- Taxonomy of formal methods.
- Transformation vs. reactive vs. hybrid systems.
- Automata theory.
- State-based development methods.
- State chart and activity chart.
- (e.g.) Statemate semantics and development.
- Real-time aspects in (e.g.) Statemate.
- Case studies.

PREREQUISITES: None

RECOMMENDED ASSESMENT: Coursework and unseen paper