Lecture 1 - January 6

Syllabus & Introduction

Safety-Critical Systems
Verification vs. Validation
Theorem Proving vs. Model Checking
TLA+

Course Learning Outcomes (CLOs)

CLO1 Explain the importance of safety-, mission-, business-, and security-critical systems.

CLO2 Demonstrate knowledge of the importance of good software engineering practices for critical systems.

CLO3 Use rigorous software engineering methods to develop dependable software applications that are accompanied by certification evidence for their safety and correctness.

CLO4 Demonstrate knowledge of the method and tools using deductive approaches (such as theorem proving).

CLO5 Demonstrate knowledge of methods and tools for algorithmic approaches (such as model checking, bounded satisfiability) etc.

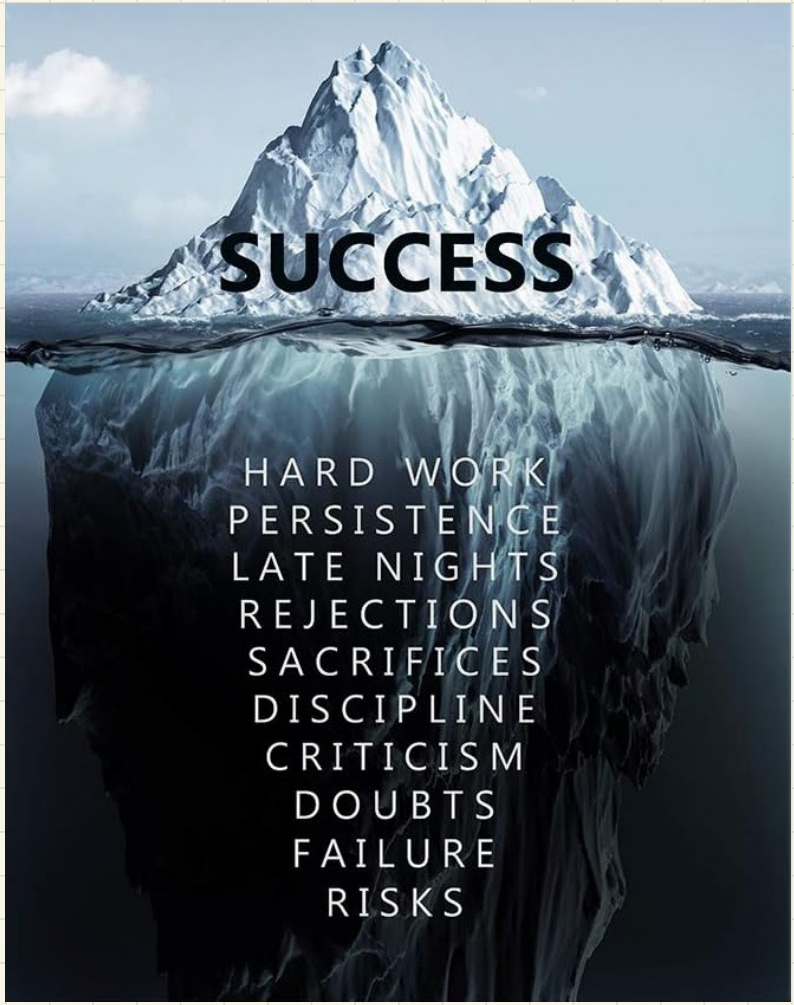
CLO6 Demonstrate knowledge of the theory underlying deductive and algorithmic approaches.

CLO7 Use industrial strength tools associated with the methods on large systems.

Exam
- ↳ 3 hours
- ↳ cumulative
- ↳ allowed to use a data sheet
- ↳ mostly short answer questions (no multiple choices)

Programming Tests
- ① submitted "code" should compile
- ↳ in-person
- ↳ TLA+ toolbox (Lab1) Pluscal (partial marks possible)
- ② syntax guide available during test.
- ↳ similar to lab exercises

Written Tests
- ↳ mostly multiple choice (one or more correct answers).
- ↳ not cumulative
- ↳ eClass (in-person)



General Tips about Success

Source: https://a.co/d/aQ13fR1

Safety Critical Systems (SCS)

- ↳ auto-pilot / auto driving
- ↳ traffic light / train gate
- ↳ air bag deployment.
- ↳ elevator / escalator
- ↳ pacemaker (embedded system)
  - ↳ pacemaker challenge (McMaster Uni.)
- ↳ nuclear power plant
  - ↳ shutdown system