Project Specifications for “Unified Approach to V&V”

The projects will be end to end case studies in the UAVV. The process will be as follows:

1. Identify a problem of modest size and develop an English narrative problem description.
2. Write and justify an informal set of property specifications for the problem. “Justify” means specifying why this set of properties leads to a robust or secure system.
3. Construct a program or model of the system with executable semantics using the design methodology prescribed for generating verifiable software. The design methodology is sketched in “Design Methodology for Verifiable Software.”
4. Write the properties in the unified property specification language.
5. Map the verification of the properties to the methods to be used for verification. For example, some properties may be best presented as preconditions and post-conditions on components and verified through use of a theorem prover or through the use of “exhaustive” testing guided by static analysis. A temporal property may be either verified by model checking using a standard model checking system or detected at runtime through evaluating the property against an event or state trace.
6. Verify the set of properties using appropriate tools. This will sometimes mean translating the original representation into a representation where there is appropriate tool support.
7. Write up a report on the degree of success obtained and give a presentation to the class on your project.

The projects require all of design, coding, analysis, writing and communication.