AE 6561: Reliable Control Software for Aerospace and Embedded Applications (3-0-3)

Course Objectives:

- Introduce to a rational approach to high-quality embedded software design.
- Leverage the fundamental principles associated with control system design (e.g. for aerospace vehicle stability and performance) and carry them over to their code implementation.
- Expose students to the practical value and engineering usage of mathematical proofs.
- Explore embedded software applications beyond "traditional" control systems.

Expected Outcomes:

- Create a new generation of control/software engineers who will design and develop higher-standard, fully documented and *independently verifiable* real-time code.
- Bridge the gap between software engineering and embedded system design Community by giving them a common intellectual ground and concrete means to communicate.

Requirements:
Knowledge of any programming language AND
[ECE 6550 or equivalent] OR [CS 6300 or equivalent] OR Instructor consent

LIST OF TOPICS

Introductory material: This series of lectures aims at presenting the auditor with basic material concerning software analysis in a safety-critical context. It also aims at showing basic limitations of software analysis through undecidability theorems.

- Specifics of embedded programs
- Software certification and certification guidelines
- Economics of software analysis
- Principles Automatic Verification
- Complexity and undecidability issues

Software and system models: These lectures present a wide variety of mathematical models aimed at representing restricted classes of software. These models have been picked (i) because they are versatile and (ii) because many of their important properties can be analyzed automatically.

- Software Systems and models
- Introduction to Logic
- Describing programs and physical systems via state-space and transition functions
    - Automata
    - Discrete difference equations
    - Continuous differential equations
    - Discrete stochastic processes
- Describing programs by means of mathematical constraints on state variables
- Stability and performance properties of systems: Lyapunov theory

Analysis methods: The core knowledge of this course will be how to extract useful properties from software and system models. The mathematical methods all revolve around the computation of reachable sets in various variable domains, using several topologies and metrics.

- Verifying Flow-graph Programs
- Verifying Flow-graph programs as they interact with physical artifacts.
- Building program proofs from specification proofs
- Building self-checking programs
- Autocoding revisited
- Software Analysis via Constraint Solving and Semidefinite Programming
- Software Testing procedures
- Combining Testing with Verification

Putting it together: We will end this course by working out a few case studies. These will be based on embedded software used in current aerospace applications. Particular emphasis will be put on writing and documenting a complete evaluation of the pieces of software under investigation.

The course will consist of two mid-term examinations and one final project.

Textbooks:

Doron Peled, Bell Labs/Lucent Technologies, Murray Hill, NJ, USA Springer-Verlag Price: $59.95 ISBN: 0-387-95106-7

Thomas Kailath: Linear Systems.