EECE693 Computers and Safety Critical Systems (3 credits)

Department of Electrical and Computer Engineering, Howard University

Instructor: Dr. Charles Kim , ckim@howard.edu, 202-806-4821, #3014 LKD

Class Time: TR 2:10 – 3:30 pm @LKD3113

Catalog Data: A computer controlled system is a combination or interrelation of hardware, software, people, and the operating environment. Making a computer system safe and secure requires coordinated activities. Unfortunately, some of the systems have been designed and placed into service with disastrous results. The basic problem is the failure of the design to correctly integrate computer technology with the time-proven engineering and safety practices that have produced successful safety-critical systems. This course intends to review the fundamental concepts of computer systems in safety-critical systems, cyber physical systems, and complex systems, and their problems in design and system safety practices. Computer controlled systems such as SCADA (Supervisory Control and Data Acquisition System) and embedded systems are particular interests of the course in learning and applying hardware/software diversity and defense-in-depth concepts and safe design practices.

Textbooks: **Required** - Practical Design of Safety-Critical Computer Systems (William R. Dunn) Reliability Press. ISBN 0-9717527-0-2

Optional - Safeware: System Safety and Computers – A guide to preventing accidents and losses caused by technology (Nancy Leveson) Addison-Wesley. ISBN 0-201-11972-2

Resources: Handouts, excerpts and other material will be provided

Class Website: WWW.MWFTR.COM/CS2.html

Classes and Assignments:

1. Lectures
2. Students presentation on assigned subjects
3. Reading material
4. Projects

Grading:

1. Assignments (40%)
2. Presentation contents: subject understanding level (20%)
3. Final Exam (30%)
4. Attendance (10%)

Tentative Class Schedule:

Week 1: Introduction
Week 2: System Safety & Safety-Critical Computer System Design
Week 3: Computer-Caused Accidents
Week 4: Risks and Computer Systems
Week 4: Computers and Risks & How Computer Fails
Week 5: Fail-Safe System & Hierarchical View of Accidents
Week 6: Fail-Operate System & Root Cause of Accidents
Week 7: Design of safe compute system &
Week 8: Human Errors and Risks
Week 9: Hazard Analysis
Week 10: Systemic Process and Defense-in-Depth and Diversity (D3)
Week 11 - 13: Accident Analyses & Software Hazard
Week 14 -16 : Projects and Project Presentation + Final Exam