CMP3206 Safety Critical System

Period per Week			Contact Hour per Semester	Weighted Total Mark	Weighted Exam Mark	Weighted Continuous Assessment Mark	Credit Units
LH	PH	TH	CH	WTM	WEM	WCM	CU
45	30	00	60	100	60	40	4

Rationale

Computers are increasingly used in systems where safety is paramount, such as transport, power systems and medical applications. An understanding of the techniques necessary to implement robust approaches has become vitally important.

Objectives

- The principal objective of this course is to give students an opportunity to acquire knowledge in the development of safety critical systems, including the theory and practice of applying safety analysis and formal specification techniques.
- Students will also gain experience in the use of such specifications in software development and testing.

Subject Content

1. ***Standards, Safety Culture and Management***
   - Standards, Conformance and IEC61508
   - Organizational Failure and MORT
2. ***Requirements Analysis***
   - Requirements, Safety Cases and SMART
   - Hazard analysis and FMECA
3. ***Risk Analysis***
   - Probabilistic risk assessment, THERP and CREAM
   - Fault Trees, Software Fault Trees and Software PRA
4. ***Software Engineering***
   - Software Requirements and MIL-HDBK-338B
   - Software Development and DO-178B
5. ***Hardware Design***
   - Fault Tolerant Architectures and the Shuttle GPCs
   - Microprocessors, PLCs and Electromagnetic Compatibility
6. ***Static and Dynamic Testing***
   - Validation, Verification and DEF STAN 00-60
   - Testing, Formal Reasoning and Mode Confusion
7. ***Human Factors***
   - Slips, Lapses and Mistakes, GEMs and Risk Homeostasis
   - Workload, Situation Awareness and CRM
8. ***Accident and Incident Analysis***
   - Incident Reporting and Analysis, Eindhoven Classification Model
   - Accident Investigation and Reporting

Recommended and Reference Books

[1] Safeware: System Safety and Computers, by Nancy G. Leveson, University of Washington (leveson@cs.washington.edu), Addison-Wesley, 1995. ISBN: 0-

201-11972-2.

[2] Computer Related Risks, by Peter G. Neumann, SRI, ACM Press Books (ACM Press / Addison-Wesley), 1995. ISBN: 0-201-55805-X.

[3] Software in Safety Related Systems, by Brian A. Wichmann, NPL, Wiley, 1992. ISBN: 0471-93474-7.

[4] Safety-Critical Computer Systems, by Neil Storey, Addison-Wesley, 1996. ISBN: 0-201-42787-7.