**AE 4376 – Accident Causation and System Safety**

**Hours:** 2-0-2

**Catalog Description:**

All engineering students should be safety literate. This course provides an in-depth examination of the multi-disciplinary issues in accident causation and system safety (prevention) across different industries.

**Prerequisites:**

None… except a strongappetite for learning.

**textbooks:**

No textbook required. Lecture notes, accident investigations reports, and published articles will be used/provided.

**Course Objectives:**

To provide the students with a solid understanding of the multi-disciplinary issues in accident causation and system safety, including:

* the anatomy of accidents across different industries, including their common features (temporal depth of causality and diversity of agency);
* fundamental failure mechanisms and causal basis of this distinctive class of adverse events;
* general system safety principles for accident prevention;
* issues in risk analysis (tools and challenges) and choice paradigms for risk-informed decisions.

The best technology transfer mode comes “wearing shoes”; by educating and engaging engineering students in the multidisciplinary issues of accident causation and system safety, this course seeks to infuse the students, the future contributors, managers, and leaders of technology-intensive or hazardous industries, with a proper safety competence, accident awareness, and safety culture before they enter the workforce. In so doing, it is hoped the course will contribute, in the long-term, one small step towards accident prevention. The end-objective of this course is to advance the common safety agenda of reducing the burden of accidents and injuries, which is significant in this and other countries, and to help build a safer society whether in the workplace, during commute, at home, or while handling any engineering product.

**Learning Outcomes:**

Students will be able to:

1. distinguish between the phenomenology and the causal basis (etiology) of accidents, and recognize the various multi-disciplinary levers for accident prevention;
2. identify fundamental failure mechanisms in a system and paths to accidents (vulnerabilities);
3. appreciate the importance of leading safety indicators, accidents pathogens and precursors, and the organizational challenges of near-miss management systems;
4. develop a working knowledge of systems safety principles, including defense-in-depth and observability-in-depth, and an ability to translate those in different contexts in support of accident prevention and sustainment of system safety;
5. critically evaluate contributions, challenges, and overview of some techniques in risk analysis.
6. Discern salient aspects of safety culture, including an in-depth knowledge of major accidents across different industries (selection of case studies).

**Grading:**

Term paper: 40%

Presentation: 25%

Weekly readings summary: 25% (two-page summary and critical assessment of weekly reading material)

Class participation: 10% (includes attendance and active, informed participation in class discussions)

Grades will be communicated weekly, and immediately following the student presentation.

**Learning Accommodations:**

If needed, we will make classroom accommodations for students with documented disabilities. These accommodations must be arranged in advance and in accordance with the ADAPTS office (http://disabilityservices.gatech.edu).

**Topical Outline:**

**I. Background and motivation**

1. From learning from accidents to teaching about accident causation and prevention
2. Highlights from the literature on system safety and accident causation: Review of major ideas, recent contributions, and challenges

**II. Anatomy of accidents**

1. Learning from the Piper Alpha accident
2. Was the Three Mile Island a “Normal Accident?”
3. An investigation of the Therac-25 accidents
4. Role of software in spacecraft accidents
5. Safety report on the treatment of safety-critical systems in transport airplanes
6. Software in military aviation and drone mishaps
7. Epidemiology of Helicopter Accidents
8. Safety in the mining industry and the unfinished legacy of mining accidents
9. Coordinability and Consistency in Accident Causation and Prevention: Formal System-Theoretic Concepts for Safety in Multilevel Systems (including the Tenerife airport disaster)

**III. Defense-in-depth, safety principles, and accident precursors:**

1. Safety barriers: definition, classification, and performance
2. Texas City refinery accident: case-study in breakdown of Defense-In-Depth and violation of the Safety-Diagnosability Principle
3. System safety principles: a multidisciplinary engineering perspective
4. Near-miss management systems and observability-in-depth: handling safety incidents and accident precursors in light of safety principles

**IV. Risk analysis, and safety culture**

1. Introduction to risk analysis: concepts, challenges, and overview of some techniques
2. On the quantitative definition of risk
3. Uncertainties in risk analysis
4. How useful is Probabilistic Risk Assessment
5. Toward risk assessment 2.0: safety supervisory control and model-based hazard monitoring for risk-informed safety interventions
6. Introduction to Cost-Benefit Analysis, ALARP, and the Precautionary Principle
7. The nature of safety culture