# AE 4376 – Accident Causation and System Safety

**HOURS:** 2-0-2

**INSTRUCTOR:** Dr. Joseph Homer Saleh
Guggenheim G-341
jsaleh@gatech.edu

**TIME:** TBD

**OFFICE HOURS:** TBD

**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:**

The course is designed for juniors, seniors, and graduate students with some exposure to or experience with systems engineering. For others, permission of the instructor is required. This is an active-learning course with little traditional lecturing.

**TEXTBOOKS:**

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

**COURSE OBJECTIVES:**

The course has four objectives:

1. To instill a proper safety culture among engineering students before they enter the workforce
2. To meet the expectations of their future employer in terms of safety culture, or be advocates for safety issues and agents of change in environments where safety might be compromised
3. To enrich the students understanding of causality (temporal depth, diversity of agency, coordinability), and in so doing, to expand the scope of accident prevention options they can conceive and consider
4. To provide the students with a solid understanding of the multi-disciplinary issues in accident causation and system safety, including:
    4.1. the anatomy of accidents across different industries, and their common features;
    4.2. fundamental failure mechanisms and causal basis of this distinctive class of adverse events;
    4.3. general system safety principles for accident prevention;
    4.4. issues in risk analysis (tools and challenges), human factors, and safety culture.

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

**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. understand 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 and challenges of some techniques in risk analysis.
6. discern salient aspects of human factors and safety culture's contributions to accidents/safety,

**GRADING:**

- Individual term paper: 40%
- Individual or Team Presentation: 25%
  Depending on the enrollment, presentations will be a team work (for a large class > 20 students), or individual work for smaller class sizes. Presentations consist in a 20-minute summary and critical assessment of an accident case study or reading material.
- Individual Weekly readings summary: 25% (short summary and critical assessment of weekly reading material)
- Class participation: 10% (includes attendance and active, informed participation in class discussions)

**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).

**COURSE STRUCTURE & RATIONALE:**

The course is structured to "go backward" in the causal chain of accidents, from accident occurrence, to the safety principles that help with their prevention, then further upstream to risk analysis and related tools for risk-informed decision-making. This approach is pedagogically engaging and supports retention and extrapolation beyond the cases examined. Following a discussion of background material, the course delves into the "anatomy of accidents" by examining accident reports and related articles in difference industries:

- The diversity of the cases examined introduces the students to the multidisciplinary issues in accident causation, and they invite a deep reflection on the concept of causality in system accidents;
- Each case study highlights a particular aspect of system accidents or failure mechanisms, and it highlights a way of examining them;
- The cases introduce in a real, applied way (instead of through traditional lecturing) the realities of system accidents as well as foundational concepts for discussing the topic (e.g., initiating event, accident precursors, accident sequence)

The purpose of this part is for the student to take ownership of the material, to identify common accident patterns across different industries, and for the class to develop a common vocabulary for discussing the subject. The "anatomy of accidents" section also helps builds anticipation for the subsequent topics, having seen how accidents happen, what principles and tools are available for accident prevention. These are covered in the subsequent section, "Defense-in-depth, safety principles, and accident precursors". Finally, we move further back in the causal chain and examine risk analysis issues and safety culture (and time permitting, decision-choice paradigm, e.g., cost-benefit analysis, efficiency, equity, and the precautionary principle). Risk analysis at its core is the imagination of failure, or anticipatory rationality applied to the possibility of adverse events. This course will nurture and develop the "imagination of failure" in engineering systems, and ways for preempting failure mechanisms from unfolding. Imagination of failure is a necessary complement to the development of design and system innovation mindset, both fundamental to engineering education.

**TOPICAL OUTLINE:**

**I. Background and motivation**

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

**II. Anatomy of accidents**

| | |
|---|---|
| A. Learning from the Piper Alpha accident | (oil and gas industry) |
| B. Was the Three Mile Island a "Normal Accident?" | (nuclear industry) |
| C. An investigation of the Therac-25 accidents | (medical/healthcare) |
| D. Role of software in spacecraft accidents | (space industry) |
| E. Safety of safety-critical systems in transport airplanes | (airline industry) |
| F. Software in military aviation and drone mishaps | (military aviation / software) |
| G. Maintenance and inspection in helicopter accidents | (helicopter industry) |
| H. Safety in the mining industry and the unfinished legacy of mining accidents | (mining industry) |
| I. Coordinability and Consistency in Accident Causation and Prevention | (formal system-theoretic) |

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

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

**IV. From risk analysis to safety culture**

A. Introduction to risk analysis: concepts, challenges, and overview of some techniques
B. On the quantitative definition of risk
C. Uncertainties in risk analysis
D. Toward risk assessment 2.0: safety supervisory control and model-based hazard monitoring for risk-informed safety interventions
E. The Human Factors Analysis and Classification System (HFACS)
F. The nature of safety culture
G. Introduction to Cost-Benefit Analysis, ALARP, and the Precautionary Principle in Risk Analysis

## ARTICLES:

**Background and motivation:**

1. Saleh, J. H., Pendley C. "From learning from accidents to teaching about accident causation and prevention: multidisciplinary education for engineering students." Reliability Engineering and System Safety, Vol. 99, Issue 1, 2012, pp. 105–113.

2. Saleh, J. H., Marais, K. B., Bakolas, E., Cowlagi, R. V. "Highlights from the literature on system safety and accident causation: Review of major ideas, recent contributions, and challenges." Reliability Engineering and System Safety, Vol 95, Issue 11, 2010, pp. 1105–1116.

**Anatomy of accidents:**

1. Pate-Cornell, E. "Learning from the Piper Alpha accident: A postmortem analysis of the technical and organizational factors." Risk Analysis, vol. 13, No. 2, 1993, pp. 215–232.

2. Hopkins, A. "Was the Three Mile Island a "Normal Accident?" Journal of Contingencies and Crisis Management, Vol. 9, No. 2, 2001, pp. 65–72.

3. Leveson, N. G., Turner, C. S. "An investigation of the Therac-25 accidents." Computer Vol. 26, No. 7, 1993, pp. 18-41.

4. Leveson, N. G. "Role of software in spacecraft accidents." Journal of Spacecraft and Rockets, Vol. 41, No. 4, 2004, pp. 564–575.

5. "Safety report on the treatment of safety-critical systems in transport airplanes". National Transportation Safety Board report, NTSB/SR-06/02. Washington, DC.

6. Foreman, V. L., Favaro, F. M., Saleh, J.H., Johnson, C.W. "Software in military aviation and drone mishaps: analysis and recommendations for the investigation process". Reliability Engineering and System Safety, Vol. 137, 2015, pp. 101–111.

7. Saleh JH, Tikayat Ray A, Zhang KS, Churchwell JS (2019) "Maintenance and inspection as risk factors in helicopter accidents: Analysis and recommendations". PLoS ONE 14(2): e0211424.

8. (*Read only up to Section 4*) Saleh, J. H., Cummings, A. M. "Safety in the Mining Industry and the Unfinished Legacy of Mining Accidents: Safety Levers and the Principle of Defense-in-Depth for Addressing Mining Hazards." Safety Science, Vol. 49, Issue 6, 2011, pp. 764–777

9. Cowlagi, R. V., Saleh, J. H. "Coordinability and Consistency in Accident Causation and Prevention: Formal System-Theoretic Concepts for Safety in Multilevel Systems." Risk Analysis, Vol. 33, No. 3, 2013, pp. 420–433.

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

10. Sklet, S. "Safety barriers: Definition, classification, and performance." Journal of Loss Prevention in the Process Industry, Vol. 19, No. 5, 2006, pp. 494–506.

11. Saleh, J.H., Haga, R. A., Favaro, F. M., Bakolas, E. "Texas City Refinery Accident: Case Study in Breakdown of Defense-In-Depth and Violation of the Safety-Diagnosability Principle". Engineering Failure Analysis, vol. 36, 2014, pp. 121–133.

12. Saleh, J.H., Marais, K. B., Favaro, F. M. "System safety principles: A multidisciplinary engineering perspective". Journal of Loss Prevention in the Process Industry, vol. 29, 2014, pp. 283–294.

13. Gnoni, M. G., Saleh, J. H. "Near-miss management systems and observability-in-depth: handling safety incidents and accident precursors in light of safety principles". Safety Science, Vol. 91, 2017, pp. 154–167.

**Risk analysis and safety culture:**
(*tentative selection, some articles from this and the following section, CBA, might be replaced*)

14. Lecture: Introduction to risk analysis: concepts, challenges, and overview of some techniques

15. Kaplan, S., Garrick, B. J., "On the quantitative definition of risk." Risk analysis, Vol. 1, No. 1, 1981, pp. 11–27.

16. Pate-Cornell, E., "Uncertainties in risk analysis: Six levels of treatment." Reliability Engineering and System Safety, Vol. 54, No. 2, 1996, pp. 95–111.

17. Favaro, F. M., Saleh, J. H. "Toward risk assessment 2.0: safety supervisory control and model-based hazard monitoring for risk-informed safety interventions". Reliability Engineering and System Safety, Vol. 152, 2016, pp. 316–330.

18. Shappell, S. A., Wiegmann, D. A. "The Human Factors Analysis and Classification System (HFACS)". Federal Aviation Administration, Report DOT/FAA/AM-00/7, February 2000.

19. Sorenson, J. N. "Safety culture: A survey of the state of the art." Reliability Engineering and System Safety, Vol. 76, Issue 2, 2002, pp. 189–204.

**Risk and Cost-Benefit Analysis (CBA):**

20. Smyth, A. W. et al., "Probabilistic benefit-cost analysis for earthquake mitigation: Evaluating measures for apartment houses in Turkey." Earthquake Spectra, Vol. 20, No. 1, 2004, pp. 171–203.

21. Melchers, R. E. "On the ALARP approach to risk management." Reliability Engineering and System Safety, Vol. 71, Issue 2, 2001, pp. 201–208.

## Videos:

1. Challenger: Go for Launch (BBC documentary, 2001)
2. CSB Safety Video: Explosion at BP Refinery (U.S. Chemical Safety Board, 2005)
3. Piper Alpha: Spiral to Disaster (American Institute of Chemical Engineers, AIChE, 2001)

**The course fosters the integration of education and research in accident causation and system safety**. In some past cases, the students were interested in working with the instructor after the course was over to further develop their term projects. These led to several publications, conference and journal articles. Some examples are provided next. The instructor encourages and supports such arrangements.

**Journal publications that came out of previous term papers:**

1. Churchwell, J. S, Zhang, K. S, Saleh, J. H. "Epidemiology of helicopter accidents: Trends, rates, and covariates". Reliability Engineering and System Safety, Vol. 180, 2018, pp. 373–384.
2. Geng, F., Saleh, J. H. "*Challenging the emerging narrative: critical examination of coal mining safety in China, and recommendations for tackling mining hazards*". Safety Science, Vol. 75, 2015, pp. 36–48.
3. Saleh, J.H. Saltmarsh, E. Favaro, F. M., Brevault, L. "*Accident precursors, near misses, and warning signs: critical review and formal definitions within the framework of Discrete Event Systems*". Reliability Engineering and System Safety, Vol. 114, 2013, pp. 148–154.
4. Favaro, F. M., Jackson, D. W., Saleh, J. H. Mavris, D. M. "Software contributions to aircraft adverse events: case studies and analyses of recurrent accident patterns and failure mechanisms". Reliability Engineering and System Safety, Vol. 113, 2013, pp. 131–142.
5. Cowlagi, R. V., Saleh, J. H. "*Coordinability and Consistency in Accident Causation and Prevention: Formal System-Theoretic Concepts for Safety in Multilevel Systems*." Risk Analysis, Vol. 33, No. 3, 2013, pp. 420–433.
6. Saleh, J. H., Cummings, A. M. "*Safety in the Mining Industry and the Unfinished Legacy of Mining Accidents: Safety Levers and the Principle of Defense-in-Depth for Addressing Mining Hazards*." Safety Science, Vol. 49, Issue 6, 2011, pp. 764–777.
7. Bakolas, E., Saleh, J. H. "*Augmenting defense-in-depth with the concepts of observability and diagnosability from Control Theory and Discrete Event Systems*." Reliability Engineering and System Safety, Vol. 96, Issue 1, 2011, pp. 184–193.
8. Hoepfer V. M., Saleh, J. H., Marais K. B. "*On the value of redundancy subject to common-cause failures: Toward the resolution of an on-going debate.*" Reliability Engineering and System Safety, Vol. 91, Issue 12, 2009, pp. 1904–1916

**Conference publications that came out of previous term papers:**

1. Zhang, K., Churchwell, J, Saleh, J. H. "Epidemiology of helicopter accidents: Inspection blind spots, geographic disparities, and pilot demographics." American Helicopter Society (AHS) 73rd Annual Forum, May 9-11, 2017, Fort Worth, Texas.
2. Churchwell, J, Zhang, K., Saleh, J. H. "Epidemiology of helicopter accidents: Trends, rates, and covariates." American Helicopter Society (AHS) 73rd Annual Forum, d May 9-11, 2017, Fort Worth, Texas.
3. Favarò, F. M., Saleh, J. H. (2013). "Observability-in-Depth: novel safety strategy to complement defense-in-depth for dynamic real-time allocation of defensive resources." ESREL 2013 conference, Amsterdam, September 29th – October 2nd, 2013.
4. Brevault, L., Favarò, F. M., Saleh, J. H. (2013). "On primitives of causality: from the semantics of agonist and antagonist to models of accident causation and system safety". ESREL 2013 conference, Amsterdam, September 29th – October 2nd, 2013.
5. Saltmarsh E., Saleh J. H., Mavris, D. "Accident Precursors: Critical Review, Conceptual Framework, and Failure Mechanisms". PSAM11 & ESREL 2012 Conference, Helsinki, Finland. June 25-29, 2012.
6. Haga R. A., Saleh, J. H., Bakolas, E. "Texas City Refinery Explosion: Case Study in Breakdown of Defense-In-Depth and Violation of the Safety-Diagnosability Principle in Design". PSAM11 & ESREL 2012 Conference, Helsinki, Finland. June 25-29, 2012.
7. Jackson, D., Favaro F. M., Saleh J. H., Mavris, D. "Software Contributions to Aircraft Accidents and Incidents: Recent Case Studies, Analysis, and Recommendations". PSAM11 & ESREL 2012 Conference, Helsinki, Finland. June 25-29, 2012.
8. Cowlagi, R. V., Saleh, J. H. "Coordinability and Consistency in Accident Causation and System Safety: Towards a Formal Foundation of Safety in Multilevel Socio-technical Systems." European Safety and Reliability Conference (ESREL 2010), Rhodes, Greece. September 5-9, 2010.
9. Bakolas, E. Saleh, J. H. "Augmenting the Traditional Defense-in-Depth Strategy with the Concept of a Diagnosable Safety Architecture." European Safety and Reliability Conference (ESREL 2009), Prague, Czech Republic. September 7-10, 2009.