LSC Use Only
Number: _____
Submission Date: _____
Action-Date: _____

RECEIVED
FEB 10 1997
LIBERAL STUDIES

UWUCC USE Only
Number: 96-56e
Submission Date: _____
Action-Date: App 4/15/97
Senate App 4/29/97

CURRICULUM PROPOSAL COVER SHEET
University-Wide Undergraduate Curriculum Committee

I. CONTACT

Contact Person Mr. Bob McClay Phone 3018

Department Safety Sciences

II. PROPOSAL TYPE (Check All Appropriate Lines)

__X__ **COURSE** Systems Safety
Suggested 20 character title

____ New Course* _____
Course Number and Full Title

__X__ Course Revision SA 345 Systems Safety
Course Number and Full Title

____ Liberal Studies Approval+ for new or existing course _____
Course Number and Full Title

____ Course Deletion _____
Course Number and Full Title

____ Number and/or Title Change _____
Old Number and/or Full Old Title

_____
New Number and/or Full New Title

__X__ Course or Catalog Description Change SA 345 Systems Safety
Course Number and Full Title

_____ **PROGRAM:** ____ Major ____ Minor ____ Track

____ New Program* _____
Program Name

____ Program Revision* _____
Program Name

____ Program Deletion* _____
Program Name

____ Title Change _____
Old Program Name

_____
New Program Name

III. Approvals (signatures and date)

11/11/96 Lon K. Ferguson 3/12/96
Department Curriculum Committee

Robert L. Boucek 11 Nov 96 12 FEB 96
Department Chair

Mary E. Swinker 11/11/96
College Curriculum Committee

Norlene J. Zoni 11 Nov 96
College Dean

_____
+Director of Liberal Studies (where applicable)

[signature] 2/4/97
*Provost (where applicable)

* No new resources required

Attachment E

SA 345 Systems Safety

Catalog Description

SA 345 Systems Safety Analysis **(2c-31-3sh)**

Prerequisites: SA 211, MA 217

Focuses on the evaluation of system designs using detailed system analysis techniques. Topics covered include system definition, economics of systems safety, systems safety methodology, mathematics of systems analysis including statistical methods, Boolean Algebra, and reliability. Skills gained include the ability to perform preliminary hazard analysis, failure mode and effect analysis, fault tree analysis, and exercises in the application of fault tree analysis to hardware and man/machine systems. Practical analysis work is accomplished in laboratory sessions.

SYLLABUS OF RECORD (New)

I. Catalog Description

SA 345 Systems Safety Analysis
Prerequisites: SA 211, MA 217

3 credits
2 lecture hours
3 lab hours
(2c-3l-3sh)

Focuses on the evaluation of system designs using detailed system analysis techniques. Topics covered include system definition, economics of systems safety, systems safety methodology, mathematics of systems analysis including statistical methods, Boolean Algebra, and reliability. Skills gained include the ability to perform preliminary hazard analysis, failure mode and effect analysis, fault tree analysis, and exercises in the application of fault tree analysis to hardware and man/machine systems. Practical analysis work is accomplished in laboratory sessions.

II. Course Objectives

A. Students will be able to explain the general concept of a system, system design processes and the system life cycle. They will be able to construct organizational policies for preparing system safety program plans and for conducting system safety analyses.

B. Students will be able to describe the various theories of accident causation, including newer models such as the Universal Model. They will demonstrate an understanding of concepts such as accident causes most likely and worst credible effects and the relationship of these with risk.

C. Students will be able to construct a definition of any specific system so that a system safety analysis of that system could be performed.

D. Students will demonstrate that they can perform the various analyses methods below and be able to cite the limitations and areas of application of each analyses:

1. Preliminary Hazard Analysis
2. Failure Mode and Effects Analysis
3. Hazard and Operability Studies
4. Fault Tree Analysis

E. Students will be able to utilize each of the techniques above to assess the risks associated with any technological system.

F. Students will diagram Event Trees and Cause Consequence Charts and explain how these can be used to provide useful information about system risk.

G. Students will be able to explain the methodologies associated with the following hazard analyses techniques:

1. Job Safety Analysis
2. Sneak Circuit Analysis
3. Energy Trace and Barrier Analysis
4. What If Analysis

H. Students will be able to recognize the role of Software Systems and be able to identify analysis techniques that can be applied to these unique systems.

I. Students will demonstrate an understanding of reliability concepts and will be able to solve mathematical reliability problems relevant to system safety.

III. Course Outline

A. Introduction (2 hours)
1. System Concepts
2. Examples of Systems
3. Relationship of System Design/Development and Safety

B. Accident Causation Models (2 hours)
1. Clarification of Terminology
2. Historical Models
3. Contemporary Models

C. Fundamentals of System Safety Analysis (2 hours)
1. Defining Systems for Analysis
2. Types of Analyses
3. Characteristics of Analyses
4. Resources Needed to Perform Analyses
5. Information Produced by Analyses

D. Preliminary Type of Analyses (2 hours)
1. Areas of Application
2. Capabilities and Limitations
3. Organizing Analysis Results

E. Reliability and Failure Mode Type of Analyses (3 hours)
1. Reliability Concepts and Problems
2. Functional Block Diagrams
3. Capabilities and Limitations of the FMEA
4. Organizing Analysis Results

F. Software Safety Analysis (2 hours)
   1. Software Systems
   2. Analysis Techniques
   3. Organizing Analysis Results

G. Human Control Functions in a Human-Machine System (2 hours)
   1. Human Functioning in System Operation
   2. Human Limitations
   3. Human Error Identification
   4. Human Error Rates

H. Hazard Analyses Techniques (2 hours)
   1. Distinguishing Characteristics
   2. Specific Techniques
   3. Areas of Application

I. Problem Solving Techniques (2 hours)
   1. Event Trees
   2. Cause-Consequence Charts

J. Introduction to Fault Tree Analysis (4 hours)
   1. Characteristics of Analysis
   2. Deductive Logic
   3. Symbology
   4. Fault Tree Construction
   5. Qualitative Interpretation

K. Quantitative Computations for Fault Tree Analysis (3 hours)
   1. Fundamental Propositions of Boolean Algebra
   2. Rationalizing the Tree
   3. Computing Probabilities

L. Concepts of Risk, Risk Assessment and Risk Management (2 hours)
   1. Review of Risk Concepts
   2. Risk Assessment
   3. Risk Management

Laboratory Exercises (Fourteen 3-hour Sessions)

Laboratory Session	Title of Exercise	Lecture Units Covered
A	Defining a System for Analysis	C
B	Introduction to Preliminary Hazard Analysis	D
C	Conclusion of Preliminary Hazard Analysis	D
D	Introduction to Failure Mode and Effects Analysis	E
E	Performing the Failure Mode and Effects Analysis	E
F	Conclusion of the Failure Mode and Effects Analysis	E
G	Introduction to Process Hazard Analysis	H
H	Conclusion to Process Hazard Analysis	H
I	Introduction to Fault Tree Analysis	J
J	Fault Tree Construction	J
K	Qualitative Interpretation of the Fault Tree	J
L	Quantitative Interpretation of the Fault Tree	K
M	Quantitative Techniques in Fault Tree Utilization	K
N	Use of Fault Trees in Risk Assessment	L

IV. Evaluation Methods

The faculty person assigned to teach this course could be one of several faculty within the Safety Sciences Department. What follows is an example of the evaluation methods and weighting used by one of those faculty:

60% Exams	There will be three (3) written exams consisting of combinations of multiple choice, true/false and matching questions.
15% Quizzes	Periodic quizzes (3 or 4) will be given. Quizzes are announced and consist of several essay questions.
15% Homework	Periodic out-of-class assignments will be given. These usually consist of problems to be solved by the student.
10% Lab Reports	Each student will prepare lab reports on each analysis performed.

The grading scale will be based on the following:

A 90-100%
B 80-89%
C 70-79%
D 60-69%
F < 60%

or, a grading curve that results in a normal distribution of grades.

V. Required Textbooks

Readings in System Safety Analysis. IUP, 6th edition (1990).

VI. Special Resource Requirements

None

VII. Bibliography

A. Current Titles

Apostalakis, G. E., et al. eds. Accident Sequence Modeling. London: Elsevier Applied Sciences, 1988.

Copi, Irving, M. Introduction to Logic. Seventh edition. New York: MacMillan Publishing, 1986.

Layton, Donald M. System Safety Including DOD Standards. Chesterland: Weber Systems Inc., 1989.

Levenson, Nancy G. Safeware. New York: Addison-Wesley Publishing Co., 1995.

Stephenson, Joe. System Safety 2000. New York: Van Nostrand Reinhold, 1991.

Thomson, J. R. Engineering Safety Assessment: An Introduction. Essex: Longman Scientific and Technical Publishers, 1987.

Vincoli, Jeffrey W. Basic Guide to System Safety. New York: Van Nostrand Reinhold, 1993.

B. Historic Titles (some of the most important work was done in this area in the 1970's and early 1980's)

Barlow, R.E. et al. Reliability and Fault Tree Analysis. Philadelphia: Society for Industrial and Applied Mathematics, 1975.

Browning, R. L. The Loss Rate Concept in Safety Engineering. New York: Marcel-Dekker Inc., 1980.

Engineering Design Handbook-Fault Tree Analysis. Washington, DC: U.S. Army Material Command, 1971.

Green, A. E. Safety Systems Reliability. Chichester, UK: John Wiley and Sons, 1984.

Hammer, Willie. Handbook of System and Product Safety. Englewood Cliffs: Prentice Hall, 1972.

Henley, G. and Kumamoto. Reliability Engineering and Risk Assessment. Englewood Cliffs: Prentice Hall, 1980.

Iredon, W. Grant, ed. Reliability Handbook. New York: McGraw Hill Book Co., 1966.

Malasky, Sol W. System Safety Planning / Engineering / Management. Second edition. Princeton: Hayden Book Co., 1984.

O'Conner, Patrick D. T. Practical Reliability Engineering. Second edition. Chichester: John Wiley and Sons, 1985.

Swain, A .D. The Human Element in System Safety - A Guide for Modern Management. London: In Com Tec, 1975.

Vesely, W. E. et al. Fault Tree Handbook. NUREG-0492. Washington, DC: Nuclear Regulatory Commission, 1981.

Course Revision: SA 345 Systems Safety Analysis

Part II Description of the Curriculum Change

1. New catalog description

SA 345 Systems Safety Analysis — 3 credits
Prerequisites: SA 211, MA 217 — 2 lecture hours
3 lab hours
2c-31-3sh

Focuses of the evaluation of system designs using detailed system analysis techniques. Topics covered include system definition, economics of systems safety, systems safety methodology, mathematics of systems analysis including statistical methods, Boolean Algebra, and reliability. Skills gained include the ability to perform preliminary hazard analysis, failure mode and effect analysis, fault tree analysis, and the application of fault tree analysis to hardware and man/machine systems. Practical analysis work is accomplished in laboratory sessions.

2. Old catalog description

SA 345 Systems Safety Analysis — 3 credits
Prerequisites: SA 111, SA 211, MA 217 — 2 lecture hours
3 lab hours
2c-31-3sh

Focuses on the evaluation of system designs using detailed system analysis techniques. Topics covered include system definition, economics of systems safety, systems safety methodology, ergonomics approaches, mathematics of system analysis including statistical methods, Boolean Algebra, and reliability. Skills gained include preliminary hazard analysis, task analysis, failure mode and effect analysis, fault tree analysis, and the application of fault tree analysis to hardware and man/machine systems. Practical analysis work is accomplished in laboratory sessions.

3. Old and new Syllabi of Record are attached.

4. Summary of proposed changes

   a. Course modifications

      Because of a proposed curriculum change which would require both SA 345 and SA 347, the elements which have been common to both courses are being removed form one or the other. Previously, SA majors were required to complete either SA 345 or SA 347. The specific changes to this course are:

i. Course elements addressing Ergonomics in design and Task Analysis have been removed form SA 345 and are concentrated in SA 347.

ii. Elements where hazard analysis is covered have been expanded. This will result in more lecture coverage for:

- Software Safety Analysis
- Energy Trace and Barrier Analysis
- Process Hazard Analysis to include Hazardous Waste Operations (HAZOP), What If, etc.
- Others as time permits

iii. Coverage of problem solving techniques such as Event Trees and Cause Consequence Charts will be expanded.

v. Laboratory exercises are also to be modified to reflect these same changes.

b. Modifications in objectives

Actually the objectives for this course have not changed. The single general objective stated in the earlier syllabus has been broken out into several more detailed objectives.

c. Justification

The justification for this change is that ABET Accreditation Standards require all students to complete a course in system safety but currently this course is optional. Students may currently elect to complete SA 347 Ergonomics which provides very cursory coverage of system safety topics. The SA Department is proposing to make both courses required which will allow us to remove ergonomic topics from SA 345 and expand coverage of important system safety concepts.

5. Liberal Studies

This is an exiting course which is <u>not</u> listed as an elective under the Liberal Studies program. This will not change. These changes will not affect any Liberal Studies requirements.

6. Letters of Support

This change will not affect other departments, therefore letters of support were not obtained.

SYLLABUS OF RECORD

I. Catalog Description

SA 345 Systems Safety Analysis 2c-3l-3sh
Prerequisites: SA 111, SA 211, MA 217

Focuses on the evaluation of system designs using detailed system analysis techniques. Topics covered include system definition, economics of systems safety, systems safety methodology, ergonomics approaches, mathematics of system analysis, including statistical methods, Boolean algebra, and reliability. Preliminary hazard analysis, task analysis, failure mode and effect analysis, fault tree analysis, and exercises in the application of fault tree analysis to hardware and man/machine systems. Practical analysis work is accomplished in laboratory sessions.

II. Course Objectives

A. Students must become knowledgeable about the concept of systems, system design processes, and the system life cycle. Students will also learn how and organization can develop a policy and provide the resources for conducting system safety analysis as well as the structure and necessary skills of the analysis team.

B. Students must be familiar with the various general theories of accident causation including newer models such as the Universal model. Concepts such as causes, most likely and worst credible effects, frequency, and severity must be learned. Students must understand the logic implicit in inductive and deductive analytical methods as well as the basis for empirical methods of hazard evaluation.

C. Students must learn assitional systems and analytical concepts including system element interaction, system element hierarchy, system bounding and the limit of resolution. Students will be able to define any particular system for analysis.

D. Through actual practice, students must master the essential techniques of the Preliminary Hazard Analysis and must understand its range of application, and its limitations.

E. Students must gain a basic understanding of non-human element reliability; they must also know how to construct and interpret Functional Block Diagrams.

Through actual practice, students must master the essential techniques of the Failure Mode and Effects type of analysis and must understand their range of application and limitations.

F. The importance of the human element in system operation must be understood. Students must learn the extent of human limitations in the essential functions of sensing information processing, information storage, decision making and motor response. From an understanding of these limitations, students must be able to recognize and explain causes for human error.

G. Through actual practice, students must master the essential techniques of the Task Analysis and must understand its range of application and its limitations.

H. Students must learn the distinctive approach and capabilities of the Fault Tree Analysis. Through actual practice, students must master the essential techniques of the Fault Tree Analysis and must understand its range of application and its limitations. The qualitative interpretation of Fault Tree must also be understood.

I. Students must understand and gain skill in using Boolean Algebra to rationalize Fault Trees. Methods of determining the probability of the most undesired event via classical probability calculations and the Lambda Tau technique must be learned. Students must know how to use Fault Tree results in Cost-Benefit type analysis.

III. Course Outline

A. Introduction (2 hours)

B. Accident Causation Models (2 hours)

C. Fundamentals of System Safety Analysis (2 hours)

D. Preliminary Type of Analyses (2 hours)

E. Failure Mode Type of Analyses (3 hours)

F. Human Control Functions in a Man-Machine System (2 hours)

G. Ergonomics in Engineering Design (2 hours)

H. Task Analyses (2 hours)

I. Introduction to Fault Tree Analysis (6 hours)

J. Quantitative Computations for Fault Tree Analysis (5 hours)

K. Laboratory Exercises (14 3-hour sessions)

1. Defining a System for Analysis

2. Introduction to Preliminary Hazard Analysis

3. Conclusion of Preliminary Hazard Analysis

4. Introduction to Failure Mode and Effects Type Analysis

5. Performing the Failure Mode Effects and Criticality Analysis

6. Conclusion of the FMECA Technique

7. Introduction to Task Analysis

8. Performing the Task Analysis

9. Concluding the Task Analysis

10. Introduction to Fault Tree Analysis

11. Fault Tree Construction

12. Qualitative Interpretation of the Fault Tree

13. Quantitative Techniques in Fault Tree Utilization

14. Advanced Fault Tree Utilization

IV. Evaluation Methods

The final grade will be determined by using any combination of at least four(4) of the following evaluation methods within the range of weights shown as determined by the individual faculty member and which must total 100%.

0-60%	Exams	There will be a minimum of two written exams consisting of combinations of multiple choice, true/false, matching, completion, and essay questions; or other interactive exams. Make-up exams are at the discretion of the individual faculty member.
0-25%	Quizzes	Periodic quizzes will be given. Some individual faculty members may utilize unannounced quizzes. Make-up quizzes are at the discretion of the individual faculty member.
0-15%	Homework	Periodic out-of-classroom assignments will be given.
0-40%	Term Papers/ Projects	Each student will prepare formal papers or projects on a topic approved by the individual faculty member.
0-20%	In-Class Writing	Each student will prepare various assignments in class utilizing free-style writing techniques as scheduled by the individual faculty member.
0-25%	Presentations	Each student will participate in an oral presentation topic approved by the individual faculty member.
0-20%	Participation	Each student will provide active engagement in the classroom.
0-25%	Group Activity	Students will be assigned various activities requiring a collaborative effort with other students.

Extra credit can be assigned to any one of the above evaluation methods at the discretion of the instructor.

The grading scale will be based on the following:

A	90-100%
B	80-89%
C	70-79%
D	60-69%
F	< 60%

or, at the discretion of the faculty member a grading curve that results in a normal distribution of grades.

V. Required Textbooks

Readings in System Safety Analysis. IUP, 6th edition (1990).

Man-Machine Engineering. Alphonse Chapanis, Wadsworth Publishing (1966).

VI. Bibliography

Accident Sequence Modeling. G.E. Apostalakis, et al. editors. Elsevier Applied Sciences, London (1988).

Barlow, R.E. et al. Reliability and Fault Tree Analysis, Society for Industrial and Applied Mathematics, Philadelphia, PA (1975).

Browning, R.L. The Loss Rate Concept in Safety Engineering, Marcel-Dekker Inc., NY (1980).

Copi, Irving, M. Introduction to Logic, 7th edition. MacMillan Publishing, NY (1986)

Engineering Design Handbook-Fault Tree Analysis. U.S. Army Material Command, Washington, D.C. (1971).

Green, A.E. Safety Systems Reliability, John Wiley and Sons, Chichester, U.K. (1984).

Hammer, Willie. Handbook of System and Product Safety. Prentice Hall, Englewood Cliffs, NJ (1972).

Henley, G. and Kumamoto. Reliability Engineering and Risk Assessment, Prentice Hall, Englewood Cliffs, NJ (1980).

Iredon, W. Grant, editor. Reliability Handbook. McGraw Hill Book Co., NY (1966).

Layton, Donald M. System Safety Including DOD Standards, Weber Systems Inc., Chesterland, OH (1989).

Malasky, Sol W. System Safety Planning / Engineering / Management, 2nd edition. Hayden Book Co., NJ (1984).

O'Conner, Patrick D.T. Practical Reliability Engineering, 2nd edition. John Wiley and Sons, Chichester, U.K. (1985).

Swain, A.D. The Human Element in System Safety - A Guide for Modern Management. In Com Tec, London, U.K. (1975).

Vesely, W.E. et al. Fault Tree Handbook. NUREG-0492, Nuclear Regulatory Commission, Washington, D.C. (1981).