Form AR 140

Subject Description Form

Subject Code	CSE40483
Subject Title	System Safety Engineering
Credit Value	3
Level	4
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	This subject aims to provide students with a range of tools and techniques in the practical applications of system safety engineering. It explains how to design for maximum safe conditions and minimum risk of accidents. It covers both design for safety principles and safety design practices.
Intended Learning Outcomes (Note 1)	Upon completion of the subject, students will be able to: a. demonstrate a basic knowledge of the essential concepts of system safety engineering; b. describe and select the appropriate methodologies and tools for analysing safety and providing safety assurance in engineering systems; c. apply the techniques for managing and designing systems for safety; d. understand the capabilities and applications of system safety tools and the three-lines-of-defence concept; e. address the specialty issues within the topic of design for safety
Subject Synopsis/ Indicative Syllabus (Note 2)	1. <u>Introduction</u> Principles of system safety engineering. Basic terminology of safety assurance. Importance of design for safety. Examples of safety engineering as well as design for safety. 2. <u>Safety Program Planning and System Safety Design Development</u> Engineering perspectives. Planning, execution, and documentation. Safety program plan and system requirement. Hazard control requirements. Design checklist. 3. <u>System Safety Assessment Techniques</u> Definition. Risk expression. Hazard and safety assessment techniques, including but not limited to, (1) preliminary hazard analysis, (2) failure modes, (3) criticality analysis, (4) hazard and operability studies, (5) system hazard analysis, (6)fault tree analysis, (7) event tree analysis.

4. Human Factors Safety Principles
   An overview of human factors supports to safety-related system design and engineering projects, human error identification, human error shaping factors and error rates, and human reliability analysis.

5. Security for Safety-Critical Systems
   An understanding of security principles, interrelationships between safety and security, data protection, and threats and vulnerability analysis.

6. Systems Engineering for Safety
   An introduction to through-life safety, lifecycle systems analysis, and modelling, safety integrity level assignments and applications, common cause analysis, and safety hazard analysis on complex systems.

7. Integrated System Safety Assessments
   An introduction and overview of the applications of system safety assessments in the design process, system safety management activities, system safety program plan, safety assurance plan, process safety management, safety case development and review, three line-of-defence assurance, and operating and managing safety-critical systems and projects.

Teaching/Learning Methodology
(Note 3)

The lectures will cover principles of knowledge of the application of system safety engineering principles. Students will be required to relate the lecture materials with assignments and through the study of pragmatic examples and case studies, project presentations, and reports.

Self-study by students, including literature review and information searching, is required to achieve all the intended learning outcomes of the subject.

Assessment Methods in Alignment with Intended Learning Outcomes
(Note 4)

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)				
		a	b	c	d	e
1. Essay	10	√	√	√	√	
2. Test/Quiz	10	√	√	√		
3. Group Project	20	√	√	√	√	√
4. Examination	60	√	√	√	√	√
Total	100 %					

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

<table>
<tr><td></td><td colspan="2">The students' knowledge of Outcomes a through e and their performance are monitored and assessed through continuous assessments, and final examination.

For continuous assessments, the students are assessed in the form of quizzes through problem-solving, as well as assignments where students will submit short essays and project reports to reflect their understanding of the module through case studies and short projects.

Written examination at the end of the semester will be used to test the understanding and application of principles related to Outcomes a through e.

Students must pass the final examination and achieve a passing overall score/ grade to pass the subject.</td></tr>
<tr><td rowspan="6">Student Study Effort Expected</td><td>Class contact:</td><td>Average hours per week</td></tr>
<tr><td>▪ Lectures / Tutorials</td><td>3 Hrs.</td></tr>
<tr><td>Other student study efforts:</td><td></td></tr>
<tr><td>▪ Course work</td><td>3 Hrs.</td></tr>
<tr><td>▪ Self-study</td><td>3 Hrs.</td></tr>
<tr><td>Total student study effort</td><td>9 Hrs.</td></tr>
<tr><td>Reading List and References</td><td colspan="2">Essential Textbooks:

Bahr, N, (2015). System Safety Engineering and Risk Assessment, A Practical Approach, 2nd Edition, CRC Press, Boca Raton.

Gullo, L.J., Dixon, J. (2018). Design for Safety, 1st Edition. John Wiley & Sons Ltd. (ISBN: 9781118974315)

Reference Textbooks:

Bjelica, M.Z. (2023). Systems, Functions and Safety: A Flipped Approach to Design for Safety, 1st Edition. Springer. (ISBN: 9783031158230)

Development Bureau (2016). Guidance Notes of Design for Safety.

Ericson, C. A. (2016). Hazard Analysis Techniques for System Safety, 2nd Edition, New York: Wiley.

Vincoli, J.W. (2014) Basic Guide to System Safety, 3rd Edition, New York: Wiley.

Zio E. (2009). Computational Methods for Reliability and Risk Analysis, World Scientific Publishing Co.</td></tr>
</table>
