

Subject Description Form

Subject Code	COMP4435
Subject Title	Dependable Computing
Credit Value	3
Level	4
Pre-requisite	COMP3334 Computer Systems Security
Co-requisite/ Exclusion	Nil
Objectives	<ol style="list-style-type: none"> 1. Introduce to students the concept of dependability as a measure of a system's availability, reliability and maintainability 2. Equip students with knowledge on the measures and techniques to improve system dependability 3. Discuss how dependable computing techniques can be applied in practical scenarios
Intended Subject Learning Outcomes	<p>Upon completion of the subject, students will be able to:</p> <p><u>Category A: Professional/academic knowledge and skills</u></p> <ol style="list-style-type: none"> 1. Understand the elements of dependability and why it matters 2. Understand how dependability of a system can be assessed or measured 3. Apply various techniques to improve the dependability of a software system <p><u>Category B: Attributes for all-roundedness</u></p> <ol style="list-style-type: none"> 4. An ability to explain the attributes, threats and means of an information system to a wide range of audience
Subject Synopsis/ Indicative Syllabus	<p>Syllabus:</p> <ol style="list-style-type: none"> 1. <u>Overview of Dependability</u> Notion of dependability, its definition, attributes (availability, reliability, safety, security, maintainability) and measurements as well as related concepts such as errors, faults and hazard. 2. <u>Fault Avoidance and Fault Elimination</u> Role of specification (the Z language), programming standards, inspection and testing. 3. <u>Fault Tolerance</u> Fault detection, masking, containment, location, reconfiguration and recovery, redundancy. 4. <u>Secure Issues in E-commerce</u> E-commerce security breaches, including Internet Fraud and Espionage, Secure Electronic Transactions (SET), the iKP protocols. 5. <u>Advanced Topics</u> Dependability evaluation techniques and tools: fault trees, Markov chains; fault tolerance in distributed systems; Information Redundancy; Risk Analysis, Disaster Recovery, Emergency Management; Security Policies, Procedures, Frameworks.
Teaching/Learning Methodology	During the lectures, students will come across the common concepts and theories. Those concepts and theories would be explained with reference to case studies.

	In the tutorials, students will be given scenarios related to the area of information security where these concepts are relevant.					
Assessment Methods in Alignment with Intended Subject Learning Outcomes	Specific Assessment Methods/Tasks	% Weighting	Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)			
			1	2	3	4
	1. Continuous Assessment	55%	✓	✓	✓	✓
	2. Examination	45%	✓	✓	✓	✓
	Total	100%				
	Types of assessments included assignments, test and examination. Assignments are designed to reinforce the concepts and theories learned in the lecture and tutorial, by solving bigger problems. Test and examination are used to assess independent problem solving and critical thinking skills.					
Student Study Effort Expected	Class contact:					
	• Lecture					39 Hours
	Other student study effort:					
	• Assignments, self-study, text and exam preparation					66 Hours
	Total student study effort:					105 Hours
Reading List and References	Reference Books: 1. John Knight, <i>Fundamentals of Dependable Computing for Software Engineers</i> , Chapman and Hall/CRC, 2012. 2. John D. Musa, <i>Software Reliability Engineering: More Reliable Software Faster and Cheaper</i> , Authorhouse, 2004.					
Last Updated	July 2016					
Prepared by	Dr Allen Au (COMP Department)					