Calendar /Course Description
Students are introduced to the different software process models and management of modular inter-communication, software engineering tools, software testing and project management including resource estimation, team organization and review. Students learn software engineering techniques for dependable and secure systems, reliability engineering, software evolution, software maintenance, quality management, configuration management, reuse and ethical issues in software engineering.

Course/Learning Outcomes
Upon successful completion of the course, the student will demonstrate the ability to:

1. Explain the different practices that are key components of various process models.
2. Apply the basic principles of software project management in a team environment.
3. Understand a variety of strategies to the testing of simple programs.
4. Identify the principal issues associated with software evolution and explain their impact on the software lifecycle.
5. Identify methods that will lead to the creation of a software architecture that achieves a specified level of reliability, dependability and security.
6. Demonstrate the understanding of ethical issues in software development

Prerequisites
COMP 2920 Software Architecture and Design

Recommended Texts/Materials
### Syllabus

<table>
<thead>
<tr>
<th>Topic #</th>
<th>Chapter Title</th>
<th>Chapter #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Software processes</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Agile software development</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Software Testing</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>Software Evolution</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Dependability and security</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Security Engineering</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Resilience engineering</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>Software Reuse</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>Project management</td>
<td>22</td>
</tr>
<tr>
<td>10</td>
<td>Project planning</td>
<td>23</td>
</tr>
<tr>
<td>11</td>
<td>Quality Management</td>
<td>24</td>
</tr>
<tr>
<td>12</td>
<td>Configuration management</td>
<td>25</td>
</tr>
<tr>
<td>13</td>
<td>Computer Reliability and Ethical Issues</td>
<td>Instructor notes</td>
</tr>
<tr>
<td>14</td>
<td>Professional Ethics and The ACM Code SE code</td>
<td>Instructor notes</td>
</tr>
</tbody>
</table>

### ACM / IEEE Knowledge Area Coverage

**IEEE Knowledge Areas that contain topics and learning outcomes covered in the course**

<table>
<thead>
<tr>
<th>Knowledge Area</th>
<th>Total Hours of Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE/Software Processes</td>
<td>3</td>
</tr>
<tr>
<td>SE/Software Project Management</td>
<td>2</td>
</tr>
<tr>
<td>SE/Tools and Environments</td>
<td>1</td>
</tr>
<tr>
<td>SE/Software Verification and Validation</td>
<td>4</td>
</tr>
<tr>
<td>SE/Software Evolution</td>
<td>2</td>
</tr>
<tr>
<td>KA</td>
<td>Knowledge Unit</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------</td>
</tr>
</tbody>
</table>
| SE | SE/Software Processes          | Systems level considerations, i.e., the interaction of software with its intended environment (cross reference IAS/Secure Software Engineering)  
  • Introduction to software process models (e.g., waterfall, incremental, agile)  
  o Activities within software lifecycles  
  • Programming in the large vs. individual programming  
  Evaluation of software process models                                                                                                        | 2      | 1      | 0              |
| SE | SE/Software Project Management |  
  • Team participation  
  o Team processes including responsibilities for tasks, meeting structure, and work schedule  
  o Roles and responsibilities in a software team  
  o Team conflict resolution  
  o Risks associated with virtual teams (communication, perception, structure)  
  • Effort Estimation (at the personal level)  
  • Risk (cross reference IAS/Secure Software Engineering)  
  o The role of risk in the lifecycle  
  o Risk categories including security, safety, market, financial, technology, people, quality, structure and process                                                                                       | 0      | 2      | 0              |
| SE | SE/Software                     |  
  • Verification and validation concepts                                                                                                                                                                                                                                                                            | 0      | 4      | 0              |
| **Verification and Validation** | • Inspections, reviews, audits  
• Testing types, including human computer interface, usability, reliability, security, conformance to specification (cross-reference IAS/Secure Software Engineering)  
• Testing fundamentals (cross-reference SDF/Development Methods)  
• Unit, integration, validation, and system testing  
• Test plan creation and test case generation  
• Black-box and white-box testing techniques  
• Regression testing and test automation  
• Defect tracking  
• Limitations of testing in particular domains, such as parallel or safety-critical systems |
| **SE** | **SE/Software Evolution** | • Software development in the context of large, pre-existing code bases  
• Software change  
• Concerns and concern location  
• Refactoring  
• Software evolution  
• Characteristics of maintainable software  
• Reengineering systems  
• Software reuse  
• Code segments  
• Libraries and frameworks  
• Components  
• Product lines |
| **SE** | **SE/Software Reliability** | • Software reliability engineering concepts  
• Software reliability, system reliability and failure behavior (cross-reference SF/Reliability Through Redundancy)  
• Fault lifecycle concepts and techniques  
• Software reliability models  
• Software fault tolerance techniques and models  
• Software reliability engineering practices |
| SF | SF/Reliability through Redundancy | - Measurement-based analysis of software reliability  
- Distinction between bugs and faults  
- Redundancy through check and retry  
- Duplication/mirroring/replicas  
- Other approaches to fault tolerance and availability | 2 |
| SDF | SDF/Development Methods | - Program comprehension  
- Program correctness  
- Types of errors (syntax, logic, run-time)  
- The concept of a specification  
- Defensive programming (e.g. secure coding, exception handling)  
- Code reviews  
- Testing fundamentals and test-case generation  
- The role and the use of contracts, including pre- and post-conditions  
- Unit testing  
- Simple refactoring | 2 |
| SP | SP/Professional Ethics | - Community values and the laws by which we live  
- The nature of professionalism including care, attention and discipline, fiduciary responsibility, and mentoring  
- Keeping up-to-date as a computing professional in terms of familiarity, tools, skills, legal and professional framework as well as the ability to self-assess and progress in the computing field  
- Professional certification, codes of ethics, conduct, and practice, such as the ACM/IEEE-CS, SE, AITP  
- Accountability, responsibility and liability (e.g. software correctness, reliability and safety, as well as ethical confidentiality of cybersecurity professionals) | 2 2 |
| SP | SP/Analytical Tools | - Forms of professional credentialing  
- Acceptable use policies for computing in the workplace  
- Ethical argumentation  
- Ethical theories and decision-making  
- Moral assumptions and values | 1 | 2 |