

Software Reliability and Safety Syllabus
Outline –

Required Texts:

Safeware - System Safety and Computers; Nancy Leveson; Addison Wesley,
ISBN 0-201-11972-2

Software Reliability Engineering 2nd Edition, John Musa , Author House, ISBN 1-
4184-9387-2

Software Measurement and Estimation, Linda Laird and M. Carol Brennan, Wiley
ISBN 0-471-67622-5

Downloadable Text (FREE):

System and Software Reliability Assurance Notebook", P. Lakey, Boeing Corp.,
A. Neufelder, produced for Rome Laboratory, 1997.

You can download this from: <http://www.softrel.com/publicat.htm>

A college level probability and statistics text....

Outline:

Case Studies and Projects will be used throughout

- 1) Overview of Trustworthy Software
 - a. Case Study: Challenger
 - b. Software Reliability and Safety
 - c. Software Reliability and Safety Engineering
 - d. Software Forensics
- 2) Definition of Necessary and Required Trustworthiness of a System
 - a. Casual Model of Accidents
 - b. Value of Availability/Reliability
 - c. Necessary Reliability
 - d. Specifying the Necessary Reliability
 - e. Safety Standards
- 3) Ethics
 - a. Case Study: SDI
 - b. Software Engineering Code Of Ethics
 - c. Parnas' "Responsibility of the Professional Engineer"
- 4) Mathematical Foundations
 - a. Basic Probability and Reliability
- 5) Hazard Analysis and Mitigation
 - a. Hazards Models
 - b. Analysis Techniques

- 6) Reliability Modeling
 - a. Reliability Block Diagrams
 - b. Cut Sets and Tie Sets Modeling
 - c. Storage Cluster Case Study
 - d. Modeling Tools
- 7) Operational Profiling and Reliability Allocation
 - a. Operational Profiles
 - b. Reliability Allocation
 - i. System
 - ii. Hardware
 - iii. Software
- 8) : Single Version Design Techniques
 - a. Fault Avoidance
 - i. Coupling and Cohesion
 - ii. Safe Languages
 - iii. Reliable Architecture Patterns
 - iv. Resilient Component Selections
 - b. Fault Anticipation
 - i. Failure Management Strategy
 - ii. Software Fault Tolerance
 - iii. Recovery and Rejuvenation
- 9) Multiple Version Design Techniques
 - a. Recovery Techniques
 - b. N-Version Controversy
 - c. Application High-Availability
 - i. Replication Techniques
 - ii. Process Replication
 - iii. Fault Tolerant Middleware and Operating Systems
 - d. Fault Insertion Testing
- 10) Prediction of Defects
 - a. Prediction vs. Estimation
 - b. Model Overview
 - c. Predicting Defect Densities
- 11) Predicting Reliability from Defects and Test Data
 - a. Predicting Failures from Defects
 - b. Estimating Failure Models
 - i. Reliability Growth
 - ii. Reliability Estimation
 - c. Tools
- 12) Reliability Assessment
 - a. Case Study:
 - i. Ability to Test Entire System
 - b. Testing Effectiveness
 - c. Types of Testing and Test Tools
 - d. Reliability Demonstration
 - e. New Research in Reliability Assessment

- 13) Security
 - a. Malware
 - i. Types of Malware and Innoculations
 - b. Outsourcing Implications
 - i. Trojan Horses
 - ii. Protecting Trade Secrets
 - c. Application Certification: Strategy and Tactics

Recommended and Referenced Texts:

<Hermann, 2000> Software Safety and Reliability: Techniques, Approaches, and Standards of Key Industrial Sectors, Herrmann, Wiley-IEEE Press; 2000 ISBN: 0769502997

<Hoffman, Weiss, 2001> Software Fundamentals, Collected Papers of David L. Parnas, Edited by Hoffman and Weiss, Addison-Wesley, 2001, ISBN 0-201-70369-6

<Lyu, 1996> Handbook of Software Reliability Engineering, by Michael R. Lyu (Editor) Publisher: McGraw Hill Text; ;) ASIN: 0070394008

<Jalote, 1998> Fault Tolerance in Distributed Systems, Jalote, Prentice Hall, 1998 ISBN 0-13-301367-7

<Marcus, Stern 2000> Blueprints for High Availability: Designing Resilient Distributed Systems, by Marcus, Stern , John Wiley & Sons;, 2000, ISBN: 0471356018

<Musa, 1998> Software Reliability Engineering by John Musa, McGraw Hill, 1998, ISBN 0-07-913271

<Neufelder, 1993> Ensuring Software Reliability, Neufelder, Dekker, 1993, ISBN 0-8247-8762-5

<Piedad, Hawkins 2000> High Availability: Design, Techniques, and Processes by Piedad & Hawkings, Prentice Hall, 2000 ISBN 0-13-096288-0

<Pullman, 2001> Software Tolerant Techniques and Implementation, Pullman, Artech House; 2001, ISBN: 1580531377

<Schneider, 1999> Trust in Cyberspace, National Academy Press, 1999 ISBN 0-309-06558-5

< Siewiorek, Swarz, 1998> Reliable Computer Systems: Design and Evaluation, by Siewiorek& Swarz, A K Peters Ltd; 1998 ISBN: 156881092X

<Shooman, 2001> Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design, by Martin L. Shooman , Wiley; 2001 ISBN: 0471293423