UNIVERSITY OF MASSACHUSETTS
DARTMOUTH

ECE454/544: Fault-Tolerant Computing & Reliability Engineering

Instructor:
Dr. Liudong Xing

Fall 2022

Welcome to ECE454/544!

- Today's lecture
  - Course Syllabus & Operational Details
  - Overview of Fault-Tolerant Computing & Reliability Engineering (FTC&RE)
  - Background Survey

Course Description

- Time: **Mon./Wed., 3:30 ~ 4:45pm**
- Mode: **Face-to-Face**
- Place: **SENG 212**

- Prerequisites
  - Probability (MTH331 or ECE 384 or equivalent)
  - Differential equations (MTH212 or equivalent)
  - Digital logic design and computer design (ECE 260)

Meet the MS CPE Math requirement

Course Outcomes

Upon successfully completing this course, you will be able to

- Demonstrate knowledge of modern techniques for designing and analyzing fault-tolerant and dependable computer-based systems
- Achieve a clear understanding of why systems fail and how they can be designed to tolerate failures and operate reliably and safely
- Develop a suitable mathematical representation of the system failure behavior
- Analyze the reliability performance of compute-based systems using appropriate models and techniques.
- Evaluate design alternatives and compare two or more systems in terms of the system reliability

Course Topics

- Concepts of fault-tolerant and dependable systems
- Fault, error, and failure cause-and-effect relationship
- Hardware redundancy techniques (passive, active, and hybrid)
- Information redundancy techniques (error detecting / correcting codes)
- Time redundancy techniques
- Software redundancy techniques (DRB, NVP, NSCP)
- Time-to-failure models & distributions
- System reliability models: fault trees, reliability block diagrams, cut/path-sets, binary decision diagrams, Markov models
- Sensitivity analysis
- Network reliability analysis
- Availability modeling and analysis

A tentative topic outline that is subject to changes based on class performance & exceptional cases

Related Courses

- ECE 560 - Computer Systems Performance Evaluation (Spring semesters; required for CPE)
  - **Responsiveness**: how quickly a given task can be accomplished by system (response time, processing time)
  - **Usage level**: how well various components of system are being used (utilization)
  - **Productivity**: how effectively a user can get work accomplished (throughput)
  - **Missionability/Dependability**: indicate if system would remain continuously operational for entire duration of a mission or how reliable the system is over the long run (reliability, MTTF, MTTR, availability) → ECE454/544
- ECE620: Dependable and Secure Computing (Spring semesters)

Resources

- Lecture notes, book chapters, and research papers
  - Available from the course website
- Reference textbooks
  - B. W. Johnson, "Design and Analysis of Fault Tolerant Digital Systems", Addison-Wesley, 1989
  - L. Xing and S. V. Amari, "Binary Decision Diagrams and Extensions for System Reliability Analysis", Wiley-Scrivener, MA, ISBN: 978-1-118-54937-7, July 2015
  - M. Rausand & A. Hoyland, "System Reliability Theory: Models, Statistical Methods, and Applications" (2nd Ed.), Wiley, 2003
  - K. S. Trivedi, "Probability and Statistics with Reliability, Queuing and Computer Science Applications" (2nd Ed.), Wiley, 2002
  - M. Modarres, M. Kaminskiy, and V. Krivtsov, "Reliability Engineering and Risk Analysis" (2nd Ed.), CRC Press, 2009, ISBN 978-0-8493-9247-4
  - M. L. Shooman, "Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design", John Wiley & Sons, 2002, ISBN 0-471-29342-3.

Course Website

- https://xingteaching.sites.umassd.edu/
  - News and announcements
  - Syllabus
  - Major deadlines
  - Homework
  - Project
  - Lecture notes
  - Exams
  - Frequently asked questions on assignments, exams
  - Check **frequently**!

Please check the class website frequently; the *Recent Posts* section will be used as a primary means of notification of new assignments, deadlines, any class related announcements and information.

Course Requirements

Homework

- Homework will be assigned pertaining to each topic. Solving problems in homework is critical to learning the material and understanding the concepts presented in the course.
- Keep each homework for helping you prepare for the exams
- Homework late policy: assignments are always due at the beginning of class on the due date. Unless you have a **legitimate** reason and inform the instructor in advance or timely, late assignments are subject to the following penalty: **assignments one day late subtract 10%; two days late loses 25%; three days late loses 50%. After 3 days the assignments will be considered a ZERO.**

Exams

- There will be two exams
  - Midterm Exam: October 17, Monday (tentative)
  - Final Exam: 3pm ~ 6pm, December 15, Thursday (See Final exam schedule at: http://www.umassd.edu/registrar/finalexams/)
- It is your responsibility to take exams at the scheduled times and to make alternative arrangements **in advance** if you have a **legitimate** reason for not being able to take an exam
- Grading concerns have expiration date (3 days)

Project for ECE544 (1)

- Investigation of technical areas that are relevant to the class and are of particular interest to yourselves.
  - Website: project description, guidelines

- Go to https://xingteaching.sites.umassd.edu/
- Click PROJECT
- Click PDF following Project Description

Project for ECE544 (2)

- Required work and deadlines
  - Team setup due Sept. 14 (Wed.)
  - Project proposal due Oct. 5 (Wed.)
  - Meeting (in-person or virtual) due Oct. 28 (Fri.)
  - Project final report due Nov. 30 (Wed.)
  - Project presentation slides due Dec. 5 (Mon.)
  - Project presentation due Dec. 5 (Mon.) & Dec. 7 (Wed.)

There is no research project for ECE454 students, but students are required to attend all the scheduled project activities (e.g., oral presentations) of ECE544 students.

Grading Policy

- ECE454
  - Homework: 20%
  - Midterm: 35%
  - Final: 45%
- ECE544
  - Homework: 8%
  - Midterm: 30%
  - Final: 42%
  - Project: 20%

In-class extra-credit problems

The letter grades will be assigned using the following approximate scale: (A+, A) [100-90] (A-, B+, B) [90-80] (B-, C+, C) [80-70] (C-, D+, D) [70-60] (D-) [60-57]] (F) [<57]

Incomplete Grade Policy

- At least 70% of the course must be already completed and an exceptional circumstance (i.e. medical issue) must exist.
- If you feel you require an incomplete for an exceptional reason, you need to email me and state your reasons for the incomplete in writing. We will then decide on a course of action.

Cancelled Classes & Exams Policy

- If class is cancelled on the day an exam is scheduled, we will have the exam the next time the class meets.
- If class is cancelled for the session prior to the exam (the day for review and for asking questions), then the next class meeting will be the "review session", and the exam will take place in the class meeting after that.

Attendance Policy

- Students are expected to regularly attend class and all other scheduled activities related to the course in person.
- The instructor reserves the right to record attendance from time to time (not regularly).
- Students who miss a lecture must self-study the missed material and make arrangement with the instructor about any questions of the missed lecture when necessary.
- Please follow the health and safety protocols when you come to the campus.

https://www.umassd.edu/covid/

Academic Integrity

- Unless specifically stated otherwise, all homework assignments and exams in this class are to be completed individually. Any collaboration with others or use of work completed by others for previous offerings of this class is considered to be unauthorized aid.
- Furthermore, you should explicitly acknowledge any sources of ideas used that are not your own; this includes other people, books, papers, web pages, etc.

Academic dishonesty will be "rewarded" with a grade of "F".

https://www.umassd.edu/studentaffairs/studenthandbook/academic-regulations-and-procedures/

In Case Of Trouble

If you feel yourself slipping behind, fell free to come and see the instructor for advice. If you do decide the class is not happening for you at this semester,

- the last day to Add/Drop is **Monday, Sept. 12**, and
- the last day to Withdraw is **Monday, Nov. 14**.

However, before you withdraw, discuss your decision with the instructor and your advisor.

In Case of Special Needs

- Please feel free to contact the instructor if you have any special needs that require accommodation.
- Particularly, if you or a family member become sick that affects your submission of an assignment or participation in an exam, please feel free to email me to request an extension to complete the assignment without late penalty or alternative arrangements for the exam.

Academic Support Services

- Academic Resource Center (www.umassd.edu/arc/)
- STEM Learning Lab (https://www.umassd.edu/arc/stemlearning-lab/)
- Writing & Multiliteracy Center (www.umassd.edu/wmc/)
- Center for Access and Success (www.umassd.edu/dss/)
- Engineering Student Support & Services (ES^3) (https://www.umassd.edu/engineering/support/)

Title IX Information

- The purpose of a university is to disseminate information, as well as to explore a universe of ideas, to encourage diverse perspectives and robust expression, and to foster the development of critical and analytical thinking skills. In many classes, including this one, students and faculty examine and analyze challenging and controversial topics.
- If a topic covered in this class triggers post-traumatic stress or other emotional distress, please discuss the matter with the professor or seek out confidential resources available from the Counseling Center, http://www.umassd.edu/counselling/, 508-999-8648 or - 8650, or the Victim Advocate in the Center for Women, Gender and Sexuality, http://www.umassd.edu/sexualviolence/, 508-910-4584.
- In an emergency contact the Department of Public Safety at 508-999-9191 24 hrs./day.

Contacting Instructor (1)

- Please feel free to contact the instructor if you have any
  - special needs
  - questions about assignments or exams
  - comments, feedbacks on how to improve lectures
  - interesting experiences or tips on how to do well in the class
- Constructive criticism will be appreciated; You may use the following Yahoo email account to send your anonymous feedback to lxing@umassd.edu
  - ID: feedback02747@yahoo.com
  - PWD: feedback4xing

Contacting Instructor (2)

- Email: lxing@umassd.edu
- Voice: 508-999-8883
- Office: SENG 213C

- Office Hours:
  - In person: M/W 2:00pm ~ 3:00pm
  - Virtual: Tue. 1:00pm ~ 3:00pm
    https://umassd.zoom.us/j/96832974567?pwd=NnRva1l6Ti9zUEx4bW52WGJPUTBIUT09
  - Or other time by appointment via email.

Enjoy the class!

Have A

Fruitful & Joyful

Semester!

Welcome to ECE454/544!

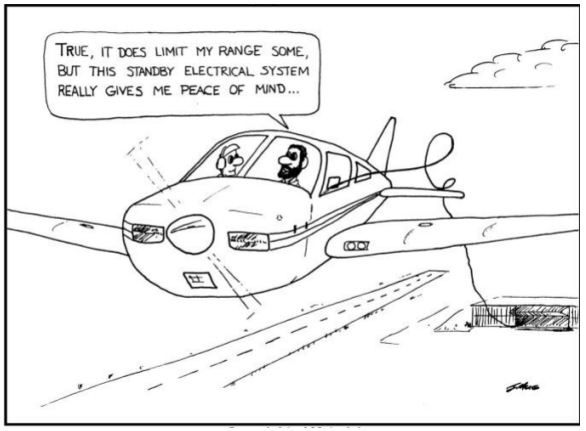
- Today's lecture
  - Course Syllabus & Operational Details
  - **Overview of fault-tolerant computing & reliability engineering (FTC&RE)**
  - Background Survey

Learning Objectives

- Explain the concept of fault tolerance and reliability
- Understand the significance of fault tolerance and reliability analysis

Fundamental Terminology (1)

- Fault-tolerant system
  - can continue to correctly perform its specified tasks in the presence of hardware failures and software errors



Fundamental Terminology (2)

- Fault-tolerance
  - the attribute that enables a system to achieve fault-tolerant operation
- Fault-tolerant computing (FTC)
  - describes the process of performing calculations, such as those performed by a computer in a fault-tolerant manner

Fault-Tolerant Techniques

- Redundancy: the addition of information, resources or time beyond what is needed for normal system operation, to detect and possibly tolerate fault
  - Hardware redundancy
  - Information redundancy
  - Time redundancy
  - Software redundancy

Fault tolerance requires the use of one or more forms of the basic redundancy types

Fault Avoidance

- Design techniques, procedures, and approaches used to prevent the occurrence of hardware and software faults.
- Examples:
  - Selecting high-quality components
  - Reviewing the designs periodically

Fault tolerance techniques handle hardware failures and software errors when they occur

Applications of Fault Tolerance

- Long-life applications
  - Exploratory space vehicles
- Critical computation applications
  - Aircraft flight control systems
  - Chemical process control
- High availability applications
  - Banking systems
  - Stock exchange computers

Reasons for Designing Fault-Tolerance into a System

- To increase the length of time a system will operate correctly
- To minimize the amount of time a system is down
- To ensure safe operation
- To meet certain design requirements
  - Reliability
  - Availability
  - Safety
  - Performability
  - Maintainability
  - Testability
  - Dependability

Basic Definitions

- Reliability, *R(t)* -- The conditional probability that a system performs correctly throughout an interval of time $[t_0, t]$, given that it was performing correctly at time t_0.
- Unreliability, *Q(t)* – [1.0 - *R(t)*]

- Fault tolerance vs. reliability
  - Fault tolerance is a technique to improve reliability

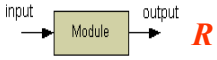
True/False?

A fault-tolerant system must have a high reliability;

A highly reliable system must be fault-tolerant.

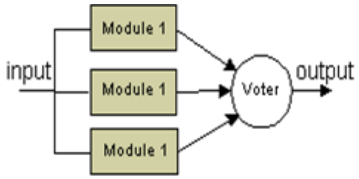
Example Fault-tolerant Design

- A simplex system

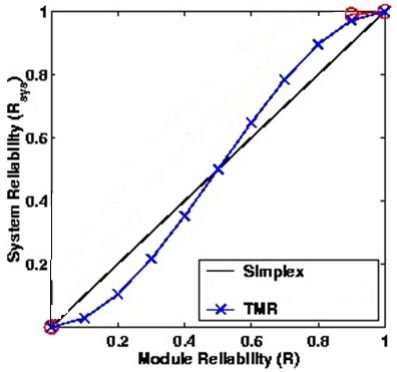


R

- A fault-tolerant design: triple modular redundancy (TMR)



Non-Fault-Tolerant vs. Fault Tolerant Designs



- When $R>0.5$, TMR is more reliable
- When $R<0.5$, TMR is worse than simplex

A fault-tolerant system may not have a high reliability;
A system with high reliability is not necessarily fault-tolerant.

True/False??

✗ A fault-tolerant system must have a high reliability

✗ A highly reliable system must be fault-tolerant

Basic Definitions (Cont'd)

- Availability, *A(t)* -- the probability that a system is operating correctly at the instant of time *t*.
  - Depends not only on how frequently the system becomes inoperable but also on how quickly it can be repaired
- Safety, *S(t)* -- the probability that a system *either* performs correctly *or* discontinues its operations in a "safe" manner.

Basic Definitions (Cont'd)

- Performability, *P(l,t)* -- the probability that a system's performance will be at or above level *l* at the instant of time *t*.
- Graceful degradation -- a system's ability to automatically decrease its level of performance when hardware and/or software faults occur.
- Maintainability, *M(t)* -- the probability that a failed system will be restored to working order within a time period *t*.

Basic Definitions (Cont'd)

- Testability
  - A **test** is a means by which the existence and quality of certain attributes within a system are determined
  - Testability – the ability to test for certain attributes within a system
- Dependability
  - A term used to encompass the concepts of reliability, availability, safety, maintainability, performability, and testability.
  - The quality of service provided by a particular system

About Reliability Engineering

- To evaluate the inherent reliability of a product or process and pinpoint potential areas for reliability improvement.
- To identify the most likely failures and then identify appropriate actions to mitigate the effects of those failures.
- To improve the product
  - A hardware/software product
  - A manufacturing process
  - A service

Established as a scientific discipline since **1950s**

Why is Reliability Important?

- Reputation
- Customer Satisfaction
- Repeat Business
- Warranty Costs
- Customer Requirements
- Competitive Advantage

http://www.weibull.com/basics/reliability.htm

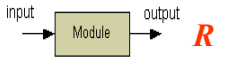
Why Reliability Analysis?

- Comparing alternative designs
- Assessing complex system reliability
- Choosing reliable system configuration
- Choosing network topology
- Reliability design considering cost

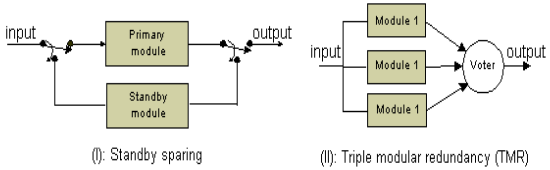
Motivating Examples

Example (1): Comparing Alternative Fault-Tolerant Designs

- A simplex system

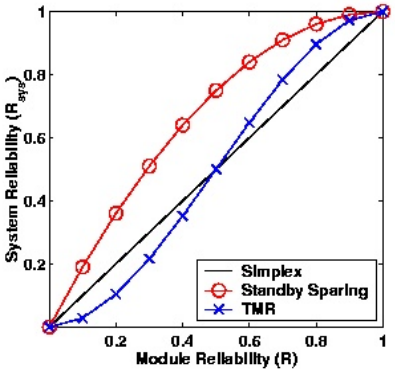


- Two alternative designs for tolerating 1 fault



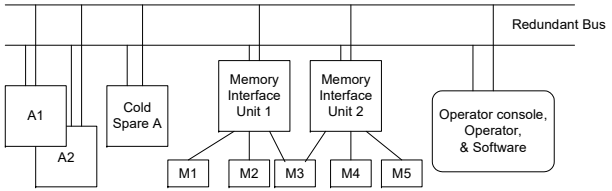
Which design is more reliable?

Example Reliability Results



- Standby sparing is the most reliable
- When $R>0.5$, TMR is better than simplex

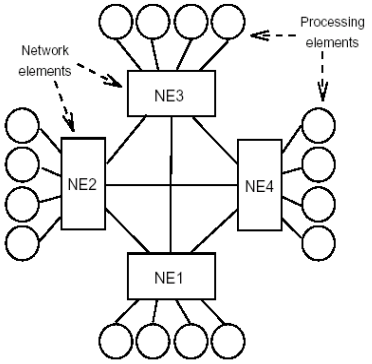
Example (2): Assessing System Reliability



- Processors A1 and A2 share the cold spare A
- 3 out of the 5 memory units are needed; if MIU fails, memory is not accessible
- At least one bus is required
- The system requires at least 1 of the three processors, at least 3 of the memory units, at least one of the redundant buses, and the operator, console and software to be operating correctly

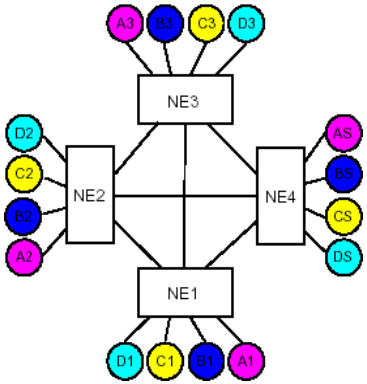
What is the reliability of the system?

Example (3) – Choosing Configuration of Fault Tolerant Parallel Processor (FTPP)



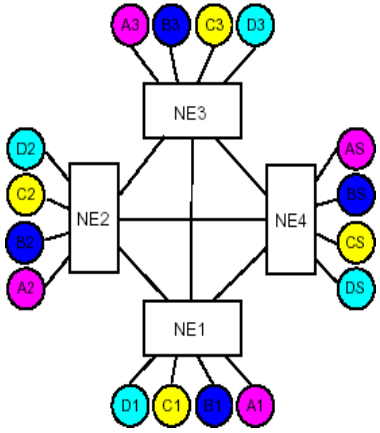
- 16 processing elements (PE), with 4 connected to each of 4 network elements (NE)
- 16 PE form 4 triads, each with a spare
- NE are fully connected
- All 4 triads must be operational to make the system operational
- And a triad fails when only one PE remains
- Consider three configurations/designs of the FTTP

FTPP Configuration #1— 1 Hot Spare per Triad



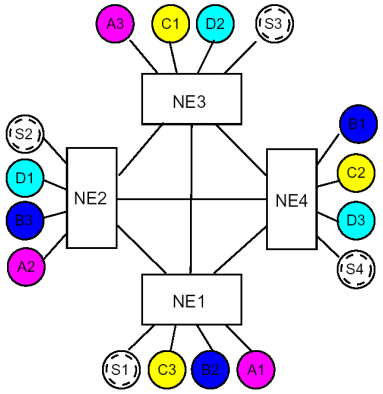
- Divides active elements of a triad among NE1, NE2, NE3; PEs in the same relative position on the first three NEs form a triad
- The PE in the same relative position on NE4 serves as a HOT spare for the triad
  - One spare for each triad
  - All spares attached to the same network element NE4

FTPP Configuration #2— 1 Cold Spare per Triad



- One COLD spare for each triad
  - keeping spares unpowered until needed
- All spares attached to the same network element NE4

FTPP Configuration #3 – One Spare Per NE



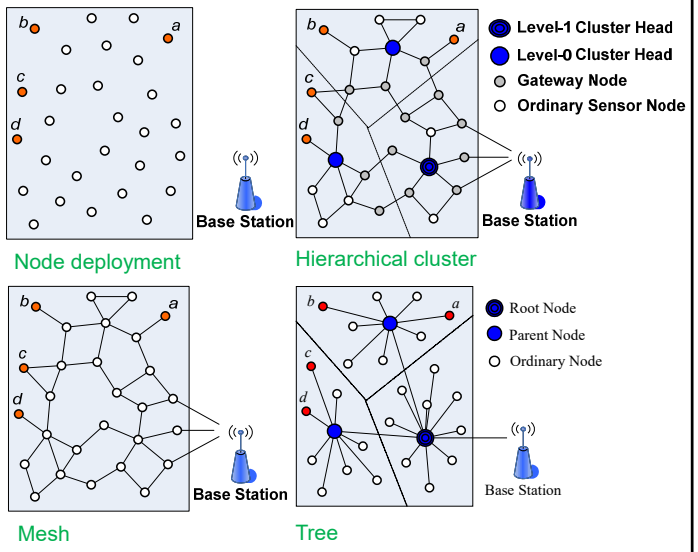
- HOT spares distributed across the NEs
- The spare element on each NE can substitute for any failed PE connected to the same NE

Summary

- Three fault-tolerant designs:
  - 1 Hot Spare per Triad
  - 1 Cold Spare per Triad
  - 1 Hot Spare per Network Element (NE)

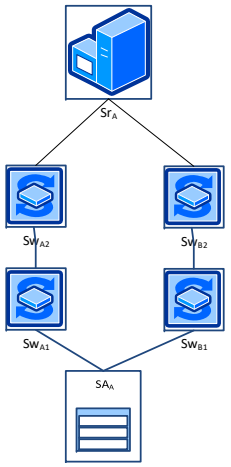
Which design is the most reliable one?

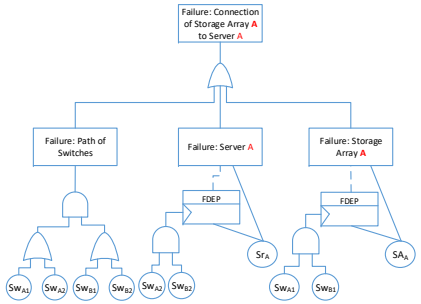
Example (4): Choosing Network Topology



Which topology design is the most reliable? Which is the least reliable?

Example (5): Reliability vs Cost

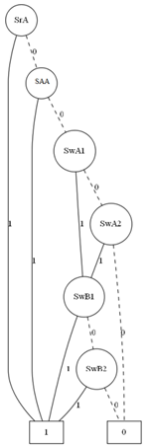




Component	Reliability
Switch	99.999%
Storage Array	99.999%
Server	97.81 %

0.0219097
(~ 8 days/year)

Sr – Server
Sw – Switch
SA – Storage Array



With doubling budget, improve the design with down time < 5 hours per year

Goals of Reliability Analysis

- Reliability analysis can
  - predict the reliability of a system for a specified period of time
  - compare alternative architecture design solution
  - facilitate trade-off studies for various fault-tolerance techniques

- Reliability analysis is a key step in the design, analysis, and tuning of fault-tolerant systems

Welcome to ECE454/544!

- Today's lecture
  - Course Syllabus & Operational Details
  - Overview of fault-tolerant computing & reliability engineering (FTC&RE)
  - **Background Survey**

Things To Do

- Check out the class website
  https://xingteaching.sites.umassd.edu/
- Review the course syllabus
  - A PDF version is available from the class website

Next Topic

- Fault, error, and failure

Welcome Again to ECE454/544!