Class2: Dependable Systems
Chapter 10

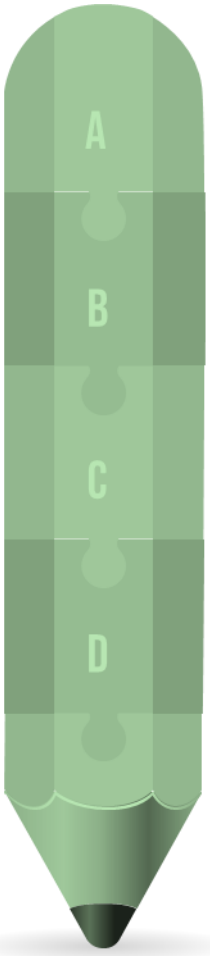
Adeeb Noor, PhD
IT Department
Faculty of Computing and Information Technology
King Abdulaziz University
Fall 2025

The Big Picture

"The dependability of systems is usually more important than their detailed functionality"

Take-home points

- The Key CLO: ″Design dependability in systems by using redundancy and diversity″
- System dependability is for business success
- Five key dimensions: Availability, Reliability, Safety, Security, Resilience
- Consider systems holistically - technical AND human
- Redundancy and diversity improve system dependability
- Formal methods help building more reliable systems
- Integrate AI tools retaining human-in-the-loop supervision



What is dependability

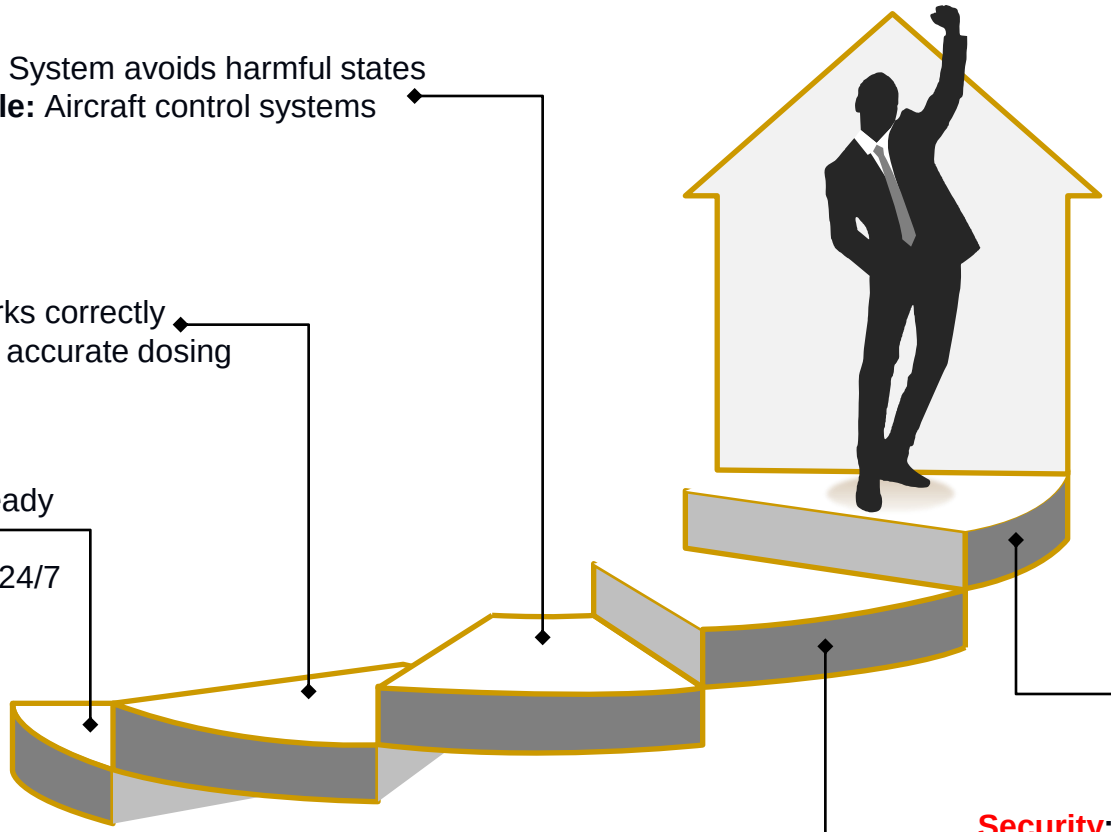
- Definition: "Capable of being trusted or depended on“*Merriam-Webster dictionary*
- Dependable System: The ability of a system to deliver service that can justifiably be trusted
- Why It Matters - Real Examples:
  - E-commerce system failures → Lost revenue
  - Car control system errors → Safety risks
- Causes of failure: hardware – software – operational

10.1 Dependability properties

Safety: System avoids harmful states
Example: Aircraft control systems

Reliability: System works correctly
Example: Insulin pump accurate dosing

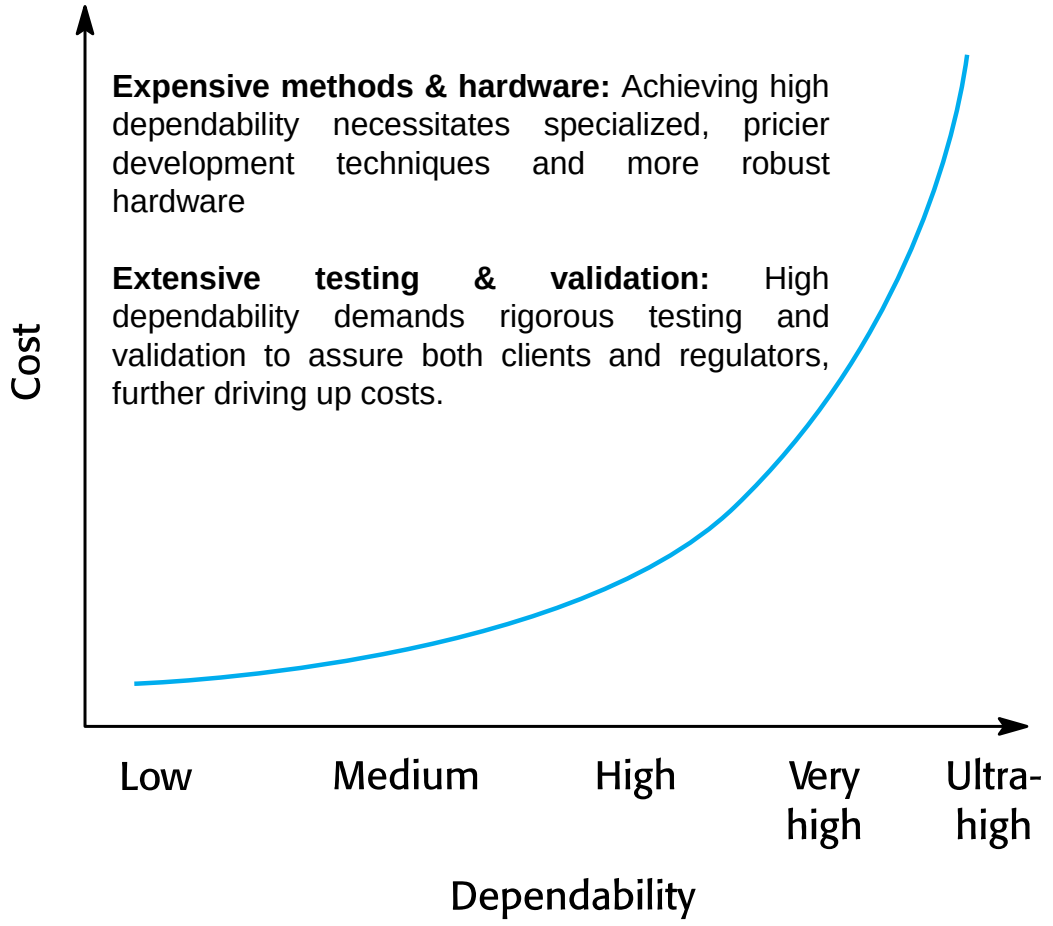
Availability: System is ready when needed
Example: ATM available 24/7



Resilience: System recovers from failures
Example: Backup power systems

Security: System resists attacks
Example: Secure against fraud

Cost/dependability curve



Because of very high costs of dependability achievement, it may be more cost effective to accept untrustworthy systems and pay for failure costs

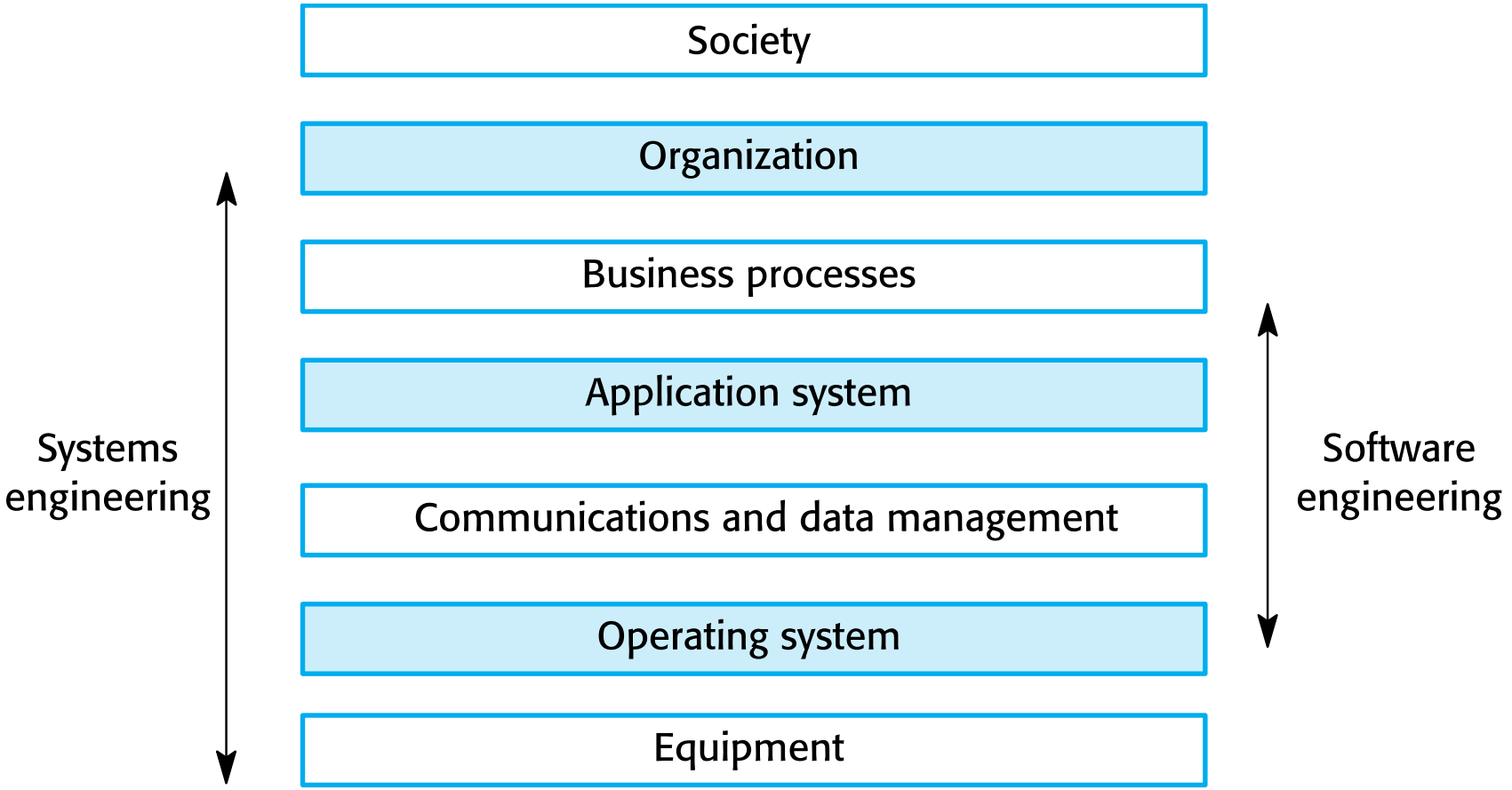
BUT

it depends on social and political factors

10.2 Sociotechnical systems

- Why cost is high; it's systems Not only software
- Software engineering is part of a larger system designed to meet human, social, or organizational needs
  - Example: Wilderness weather system ➡ (sends data like temperature, rainfall, wind speed) ➡ (Hardware: weather stations, radars) ➡ (Software: analyses data) ➡ (Forecasting Processes: creates predictions) ➡ (System Users: hikers, campers) ➡ (Organizations: government agencies, news outlets)

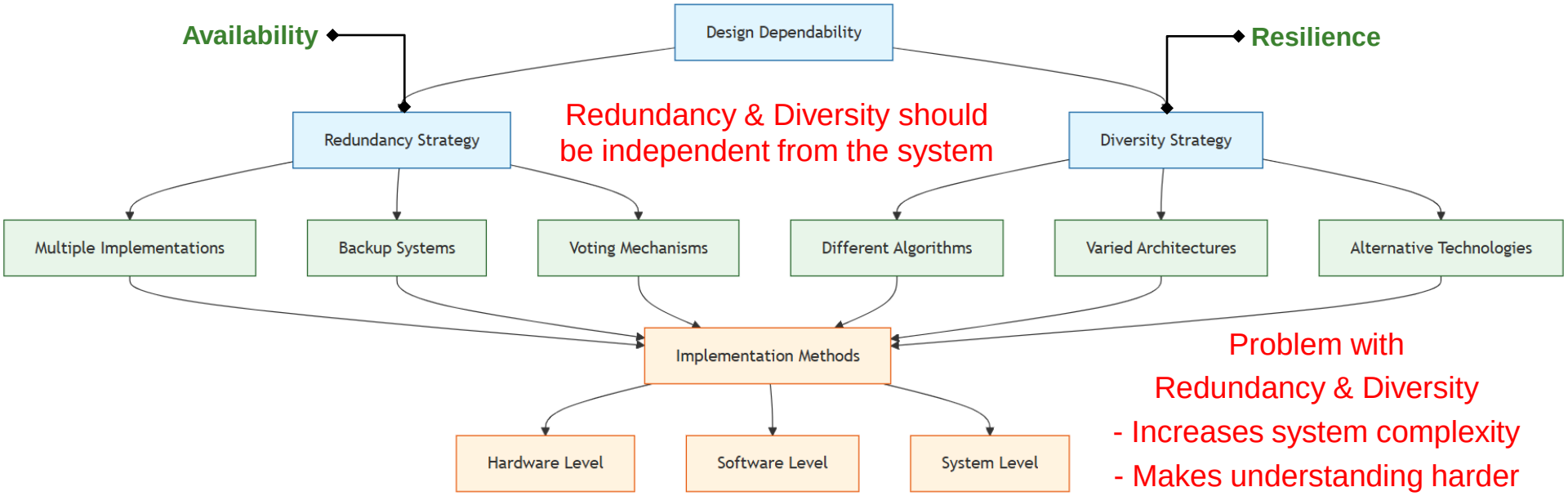
The sociotechnical systems stack



Each layer hides details from above, therefore, changes in one layer affect others

10.3 Redundancy & diversity

- Redundancy duplicates system components for backup in case of failure; Diversity different way to do the same functionality, so if one breaks, others work



Problem with Redundancy & Diversity
- Increases system complexity
- Makes understanding harder
- Requires additional functionality

10.4 Dependable processes

Dependable process activities: requirements, speciation,etc

Process characteristic	Description
Auditable	The process should be understandable by people apart from process participants, who can check that process standards are being followed and make suggestions for process improvement.
Diverse	The process should include redundant and diverse verification and validation activities.
Documentable	The process should have a defined process model that sets out the activities in the process and the documentation that is to be produced during these activities.
Robust	The process should be able to recover from failures of individual process activities.
Standardized	A comprehensive set of software development standards covering software production and documentation should be available.

10.5 Formal methods

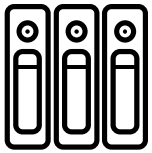
- Formal methods are approaches to software development that are based on mathematical representation and analysis of software

Key Concepts

- Mathematical approaches
- Formal model creation and analysis
- Automatic or systematic verification

Approaches

- Verification-based approaches: Checking if the program matches the blueprint
- Refinement-based approaches: Building the program directly from the blueprint

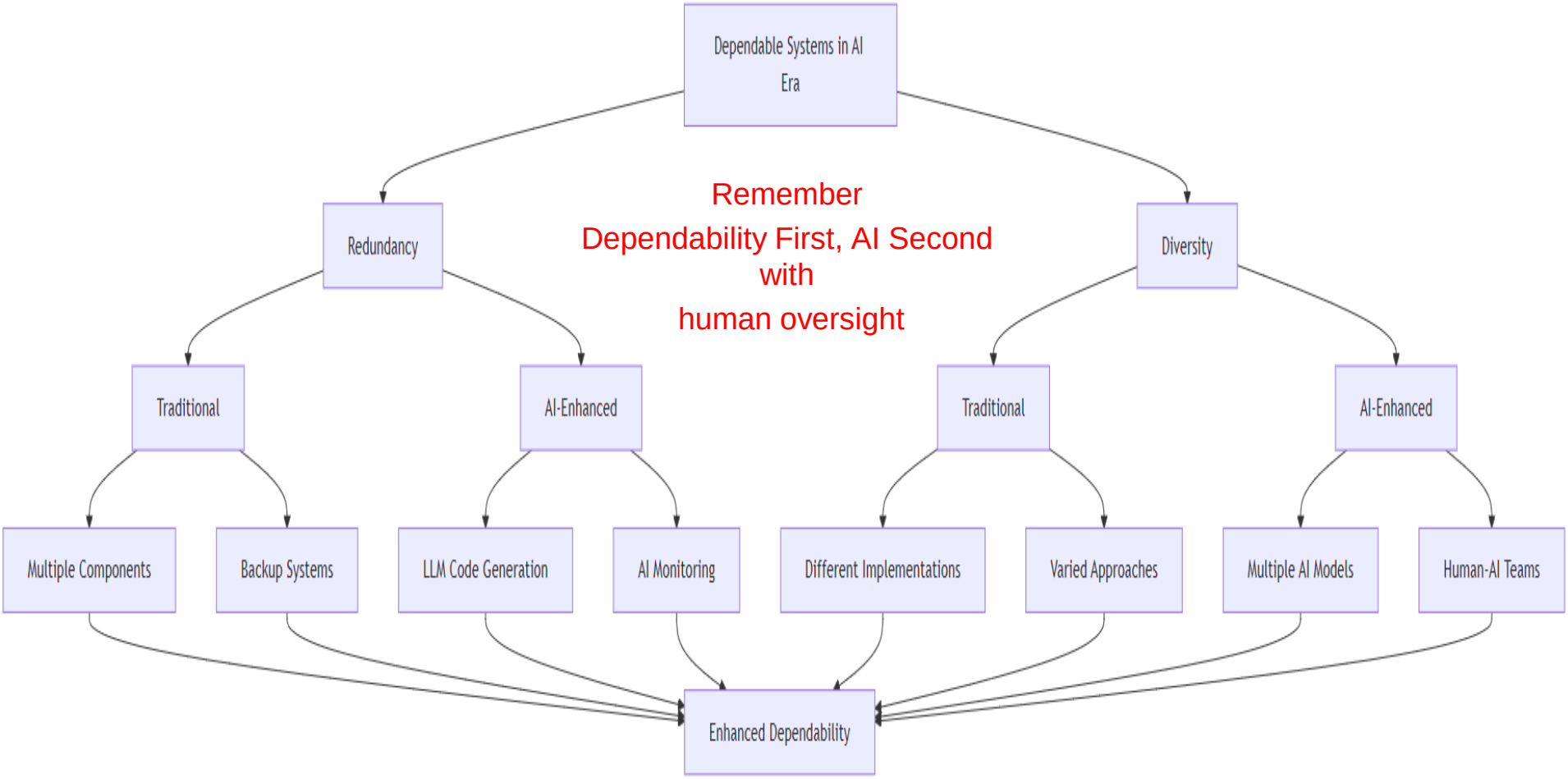


Limitations

- Problem owners don't understand formal methods
- Harder to assess the benefits
- Isn't Agile
- Software engineers are unfamiliar

A **software blueprint** is a high-level plan or outline used in the **development** of **software**

Dependable systems in AI era



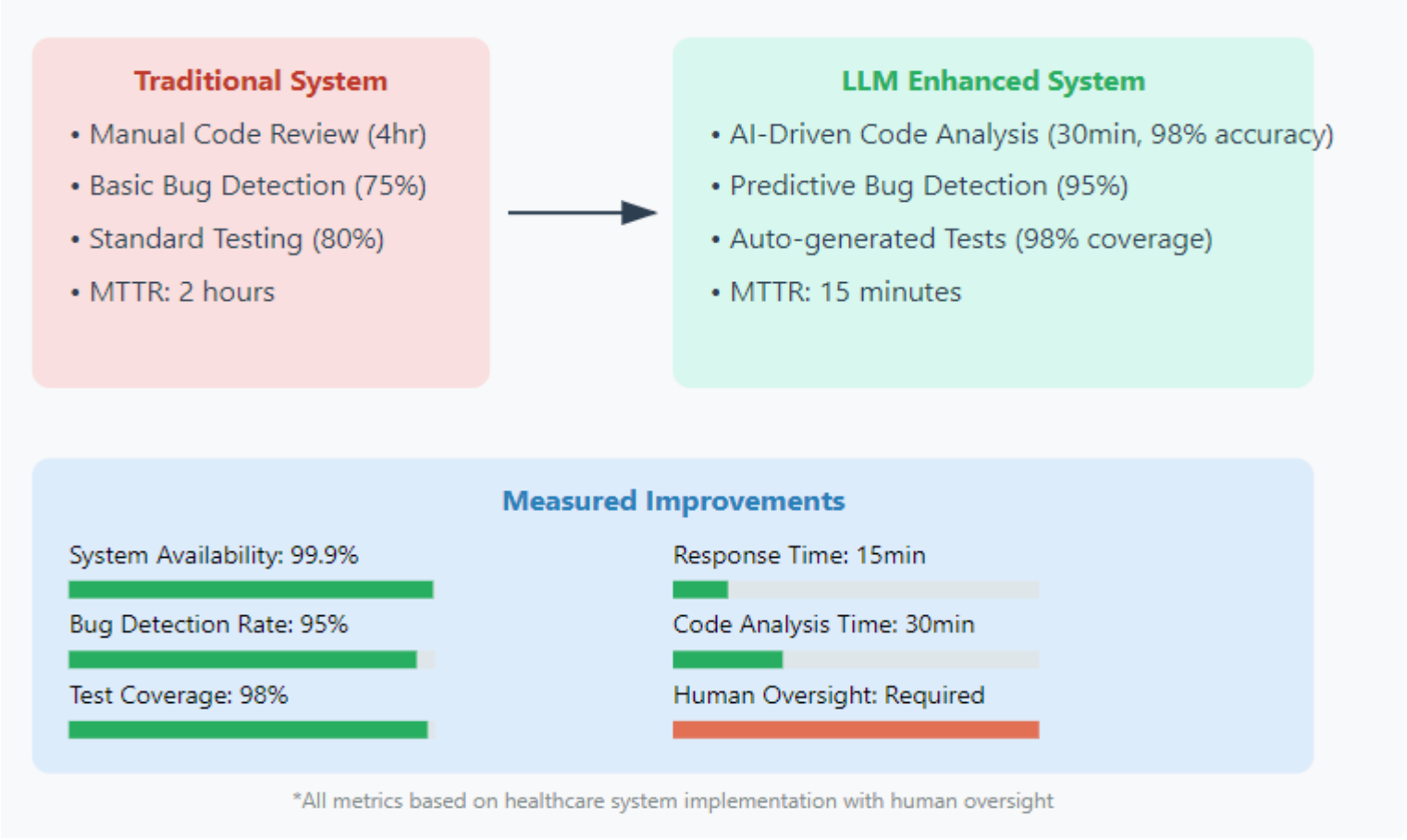
Remember

Dependability First, AI Second

with

human oversight

Ex; AI enhancement in health system dependability



To master today's lesson

- Assignment 1 is designed to assess your mastery of first (CLO): Design dependability in systems by using redundancy and diversity
- Total Marks: 5
- Submission Deadline: 8:00 PM every Saturday. No late submissions accepted
- You can use any LLM (ChatGPT, Claude, etc.)
- Collaboration allowed but submit individual work