Class6: Resilience Engineering Chapter 14

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

Today lecture topic

Lecture 4

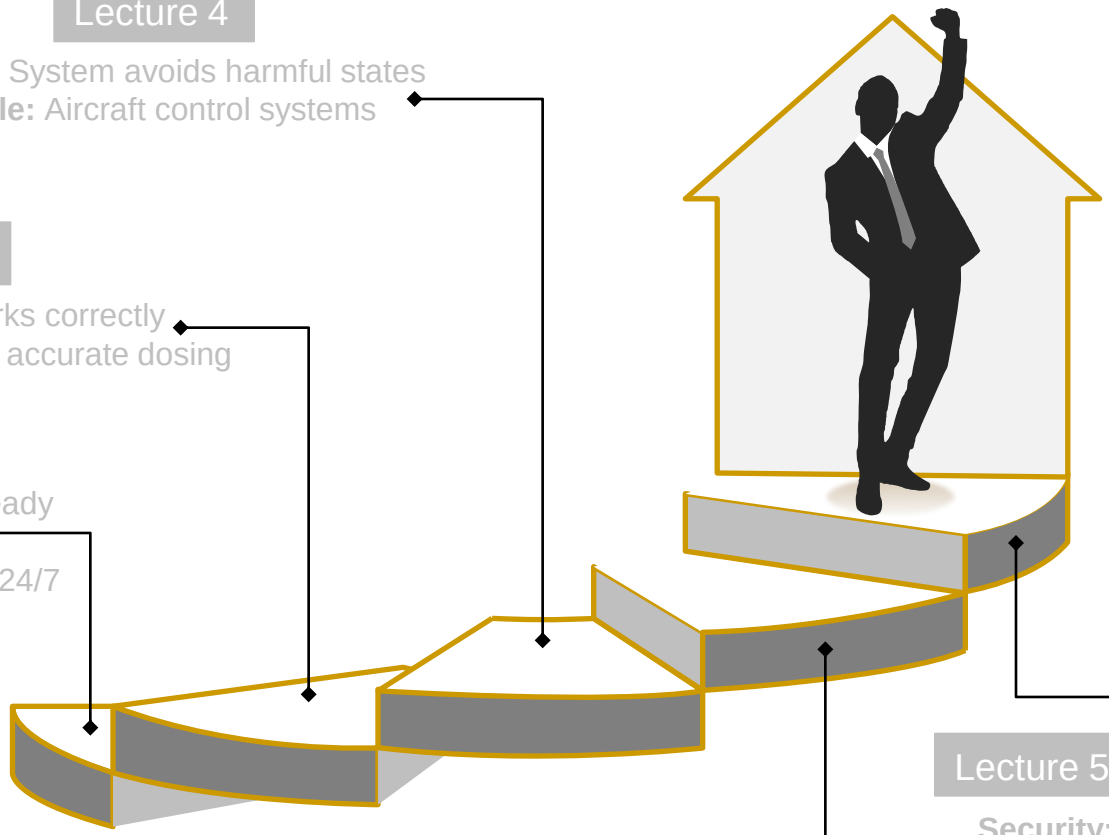
Safety: System avoids harmful states
Example: Aircraft control systems

Lecture 3

Reliability: System works correctly
Example: Insulin pump accurate dosing

Lecture 2

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



Lecture 6

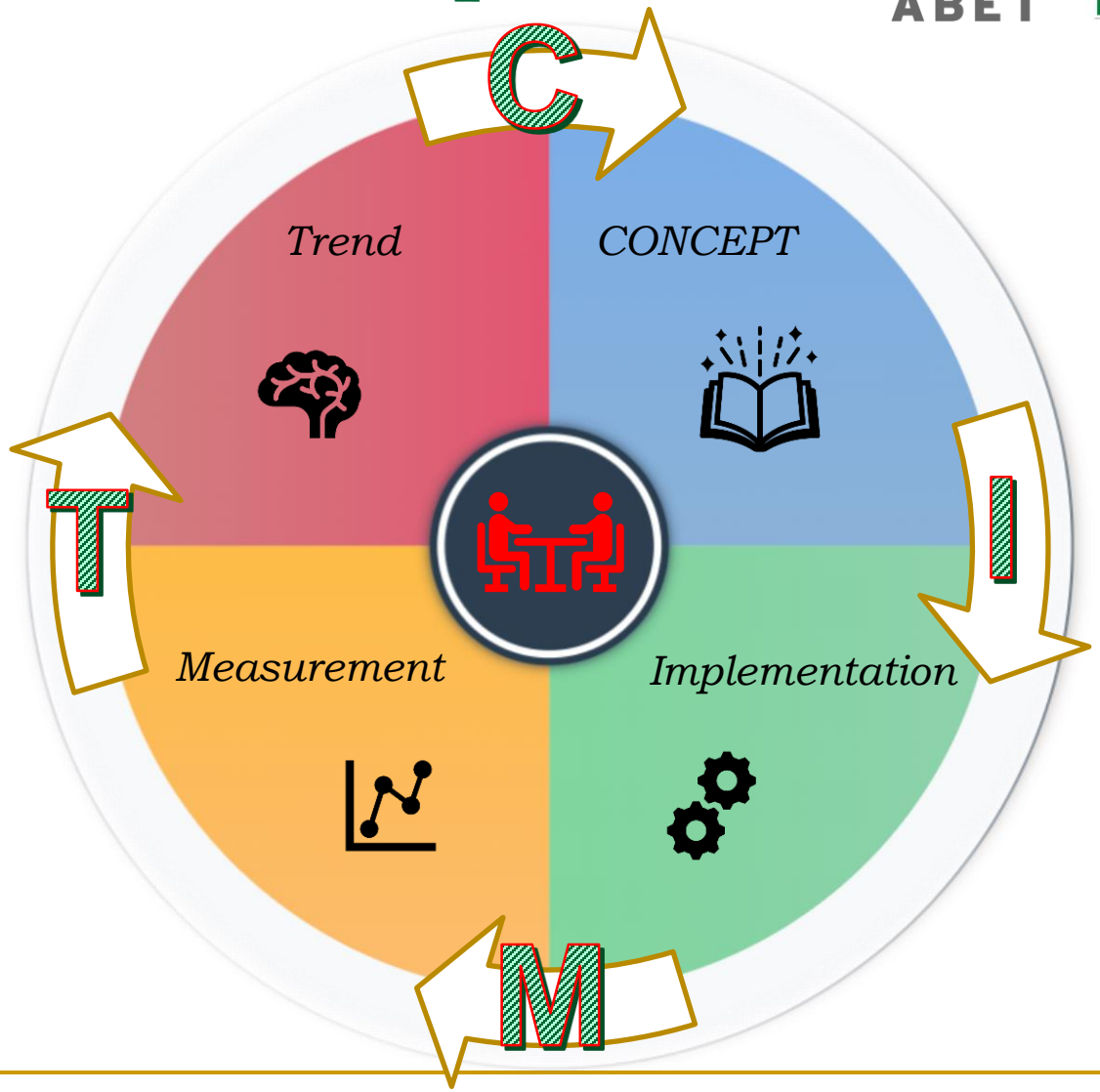
Resilience: System recovers from failures
Example: Backup power systems

Lecture 5

Security: System resists attacks
Example: Secure against fraud

CPIT-455 CIMT compass

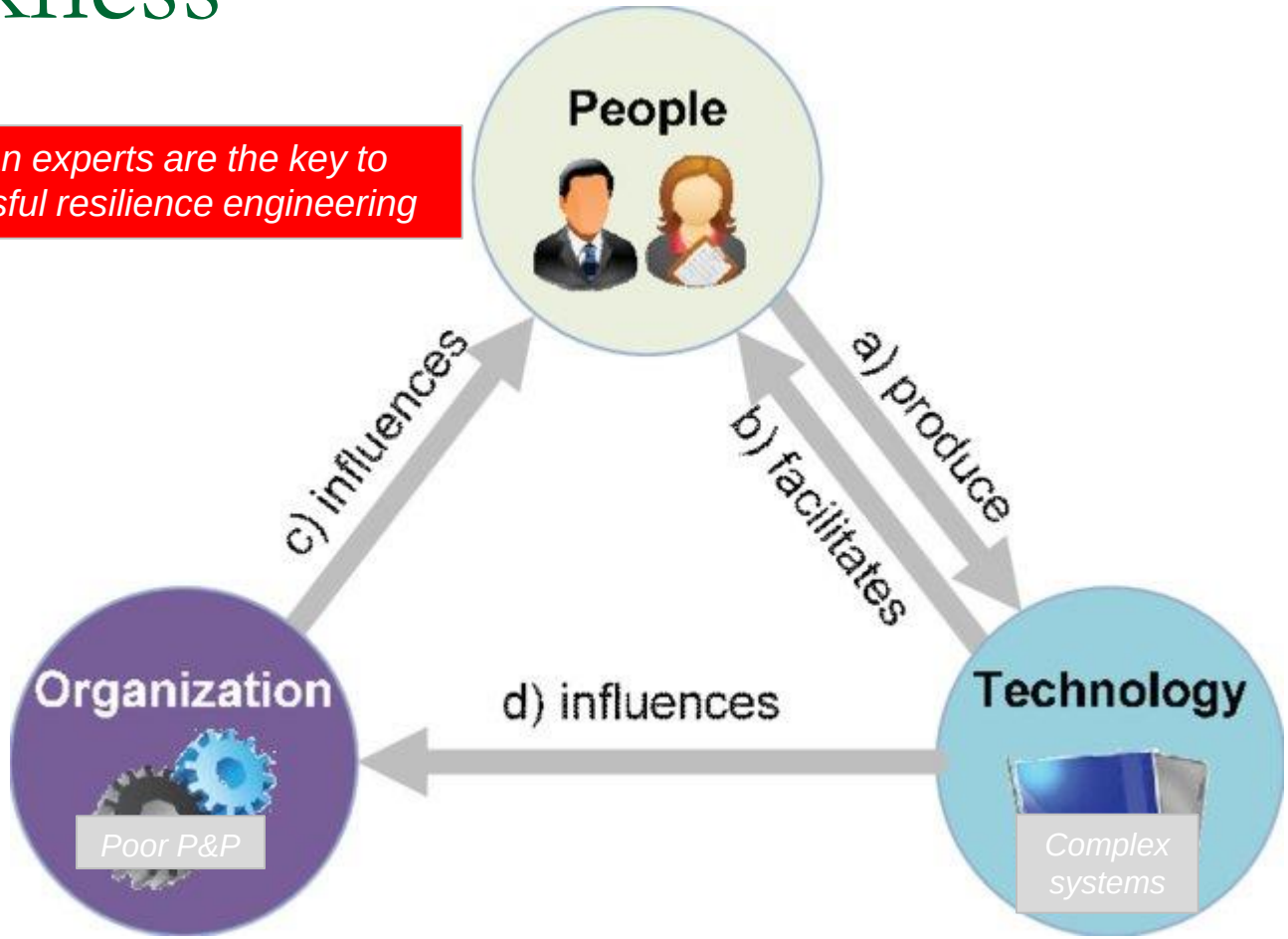
Where Academic Meets Business Reality



The big picture

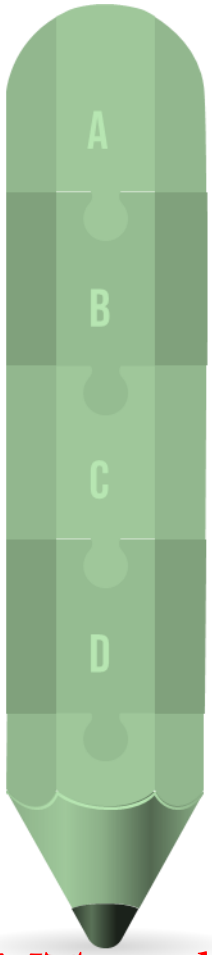
People are the foundation, not weakness

Human experts are the key to successful resilience engineering



Take-home points

- The Key CLO: Design systems to support resilience
- Cybersecurity (14.1): Cybersecurity is essential for resilience, using multiple layers to protect against attacks and minimize losses
- Sociotechnical resilience (14.2): Resilience involves human factors, organizational processes, the interaction between people and technology
- Resilient systems design (14.3): Designing resilient systems means identifying critical services, planning for recovery, and incorporating redundancy and diversity
- AI is transforming resilience engineering, but human expertise remains vital. I.e. people are the core of any resilient system; their strength and adaptability are irreplaceable



CIMT model

Chapter Summary

Resilience engineering focuses on designing and building systems that can withstand and recover from adverse events like cyberattacks and human errors, emphasizing the crucial role of human expertise in creating truly resilient systems.

Resilience: why matters

What happened:

The airline's website and mobile app were inaccessible, causing further chaos and frustration for travellers

Root Causes:

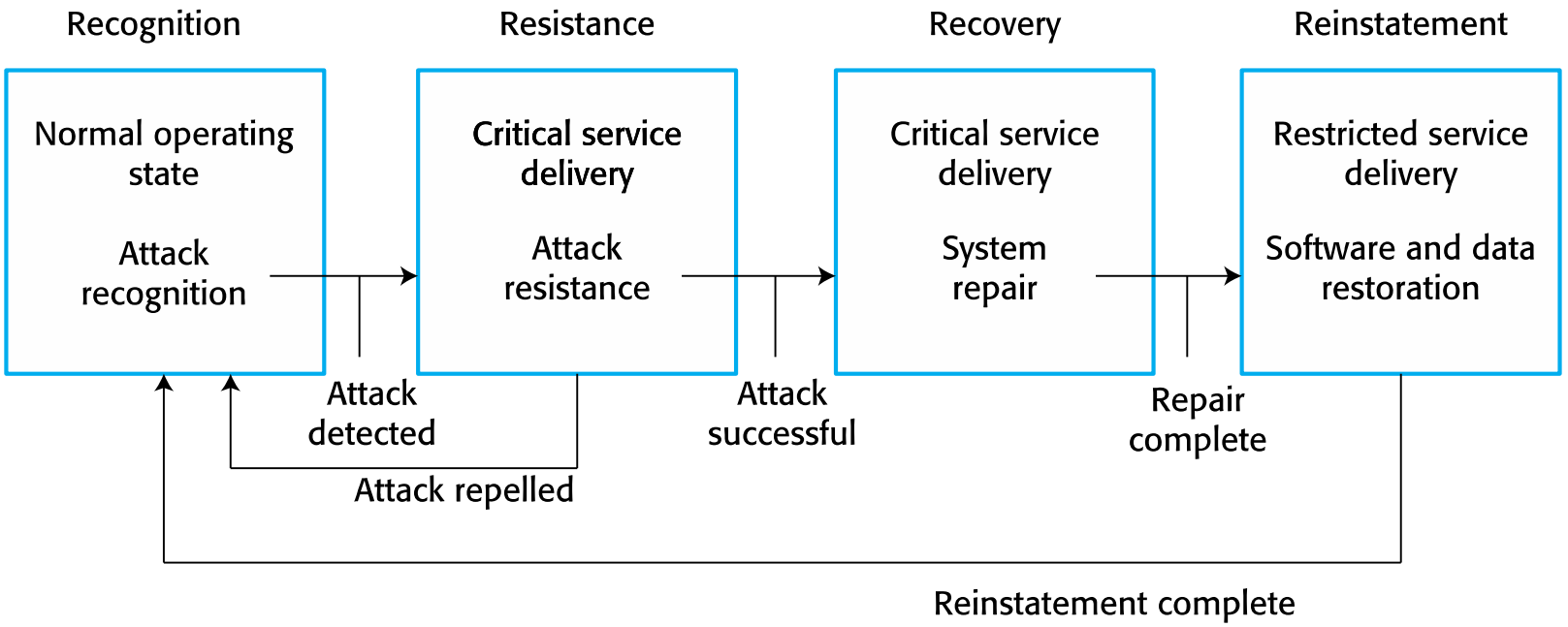
A power surge at a British Airways data center damaged systems and the backup failed to activate

How to solve Causes:

British Airways upgraded its data center infrastructure, improved backup/recovery processes, and enhanced incident management

What is resilience engineering

- The resilience of a system is a judgment of how well that system can maintain the continuity of its critical services in the presence of disruptive events



14.1 Cybersecurity

- What is it: Focuses on protecting systems and data from malicious attacks and minimizing losses in case of a successful attack

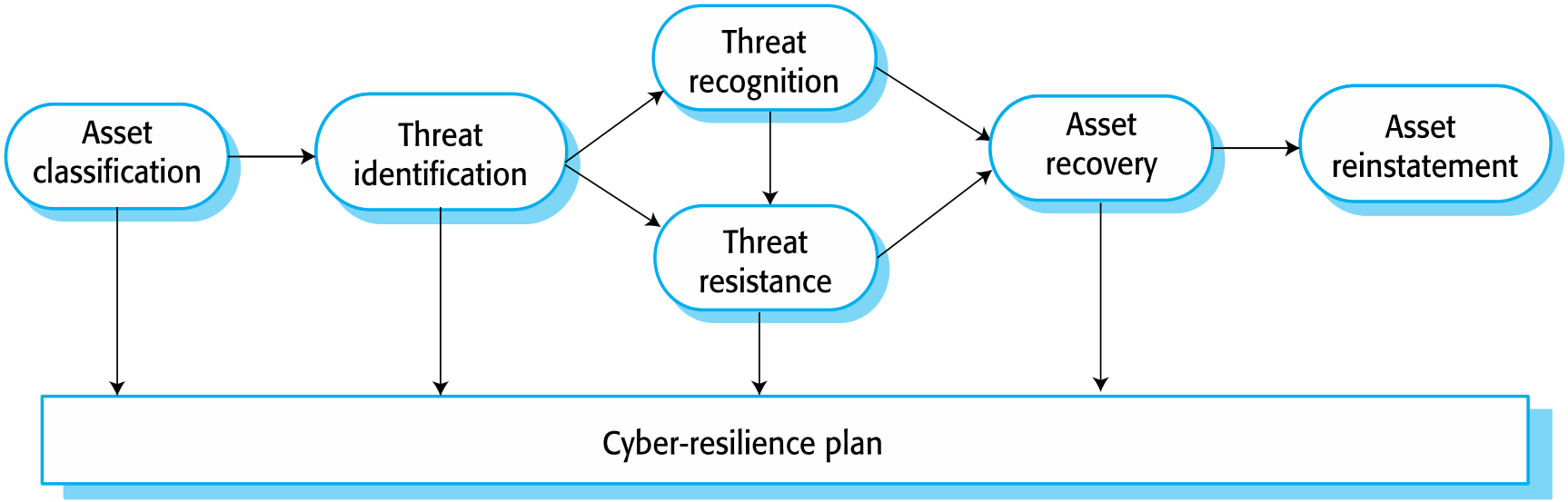
- Importance of cybersecurity in resilience engineering:
  - **Prevent disruptions**: By stopping attacks that can shut down systems (e.g., a hospital's patient database)
  - **Protect assets**: Safeguarding valuable data and infrastructure from theft or damage (e.g., a company's trade secrets)
  - **Maintain trust**: Ensuring users feel safe and confident in the system's security (e.g., online banking)
  - **Ensure business continuity**: Minimizing the impact of attacks so operations can continue (e.g., an e-commerce site can still process orders)

Cybersecurity measures - fighter

- Authentication
- Encryption
- Firewalls
- Intrusion Detection/Prevention
- Security Training
- Security Assessments
- Incident Response

Cyber-resilience planning

- A strategic framework moving from assets to threats to recovery, ensuring organizational survival through layered defences



14.2 Sociotechnical resilience

- It's People + Technology!
- Sociotechnical resilience means realizing that systems are made up of both humans AND technology.
- It's about how they work together to overcome challenges!

Why we need it:

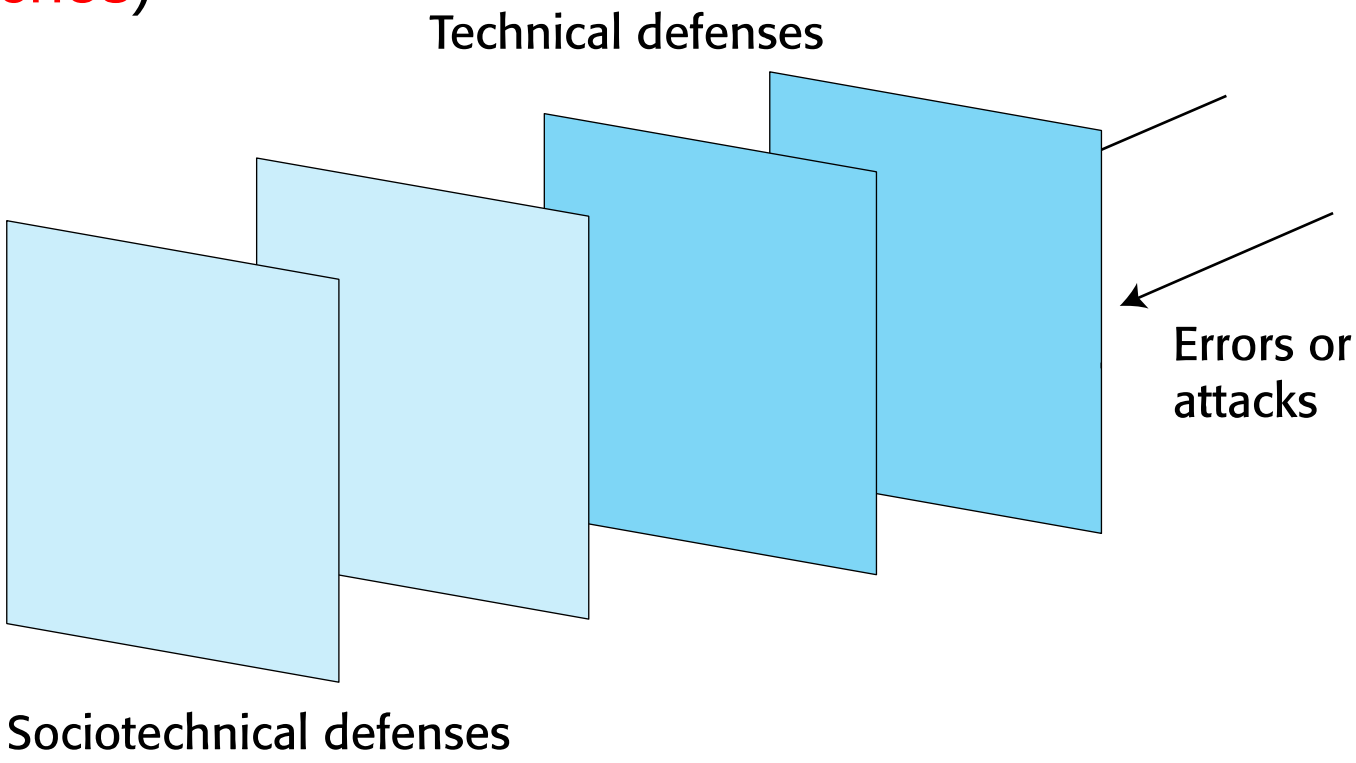
- Humans are Adaptable
- Systems are Complex
- Flexibility is Key

Characteristics of resilient organizations

- Organizations that master the cycle of responding, monitoring, anticipating, and learning from challenges

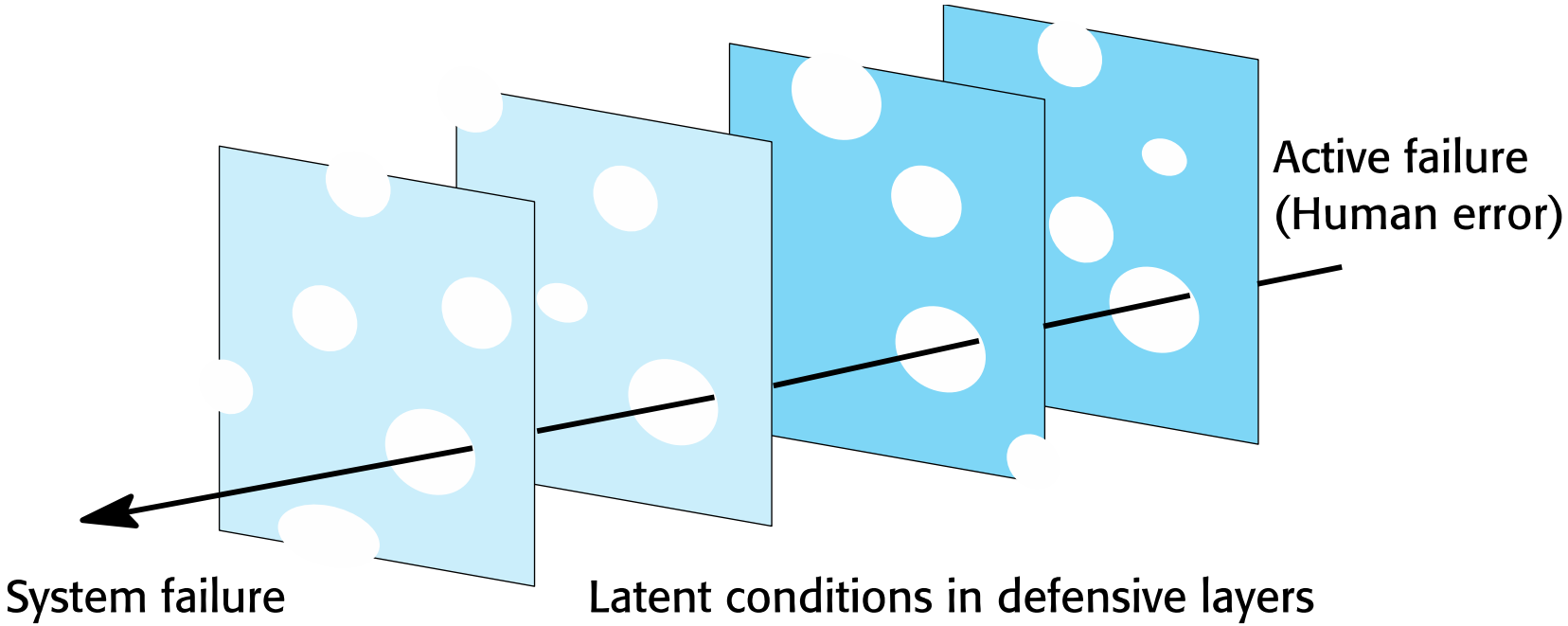
Defensive layers

- People inevitably make mistakes (human errors) that sometimes lead to serious system failures (person, system approaches)



The *Swiss Cheese* model

- Add more layers of defence (more cheese slices!)
- Make the defences different (so the holes don't line up)
- Reduce the number of holes



Operational & management processes

- Balancing Efficiency and Resilience: While efficient processes are important, they shouldn't be so rigid that they prevent people from adapting to problems

Efficient process operation	Problem management
Process optimization and control	Process flexibility and adaptability
Information hiding and security	Information sharing and visibility
Automation to reduce operator workload with fewer operators and managers	Manual processes and spare operator/manager capacity to deal with problems
Role specialization	Role sharing

The problem with automation

Too much automation can reduce resilience!

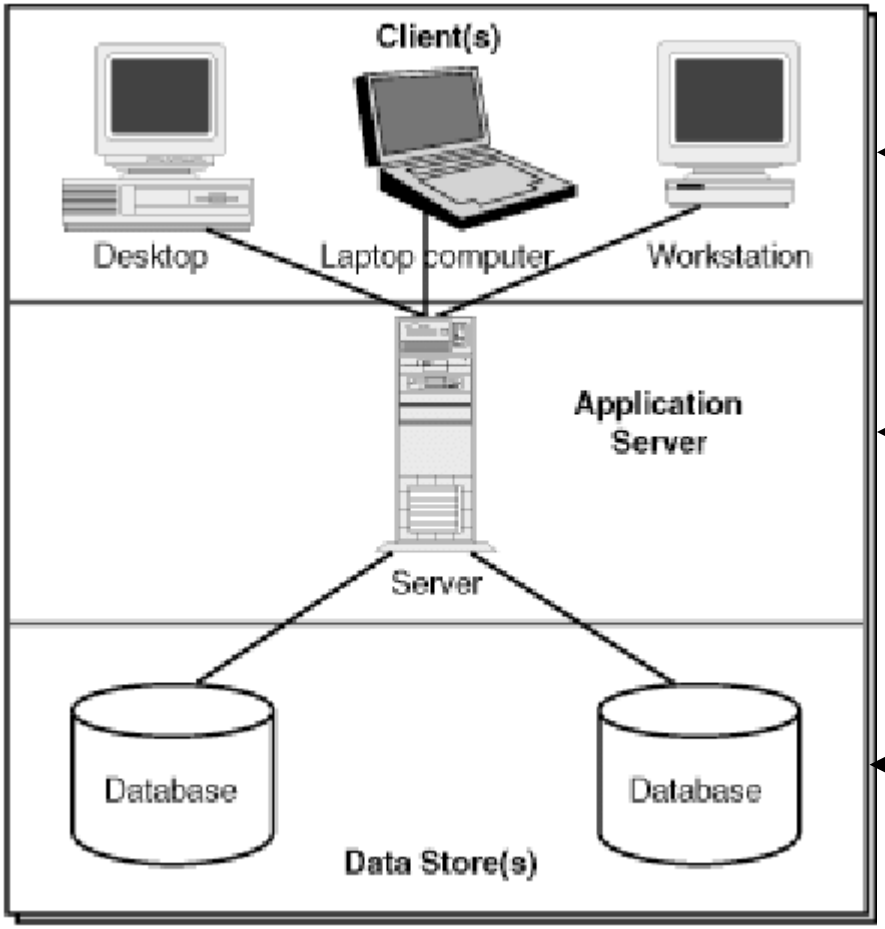
- **Automation Can Fail:** Automated systems can malfunction and make things worse
- **Reduced Human Expertise:** Over-reliance on automation can lead to a decline in human skills and experience needed to handle complex problems

14.3 Resilient systems design

Threats to the availability of assets

Threats to the integrity of assets

Threats to the confidentiality of assets



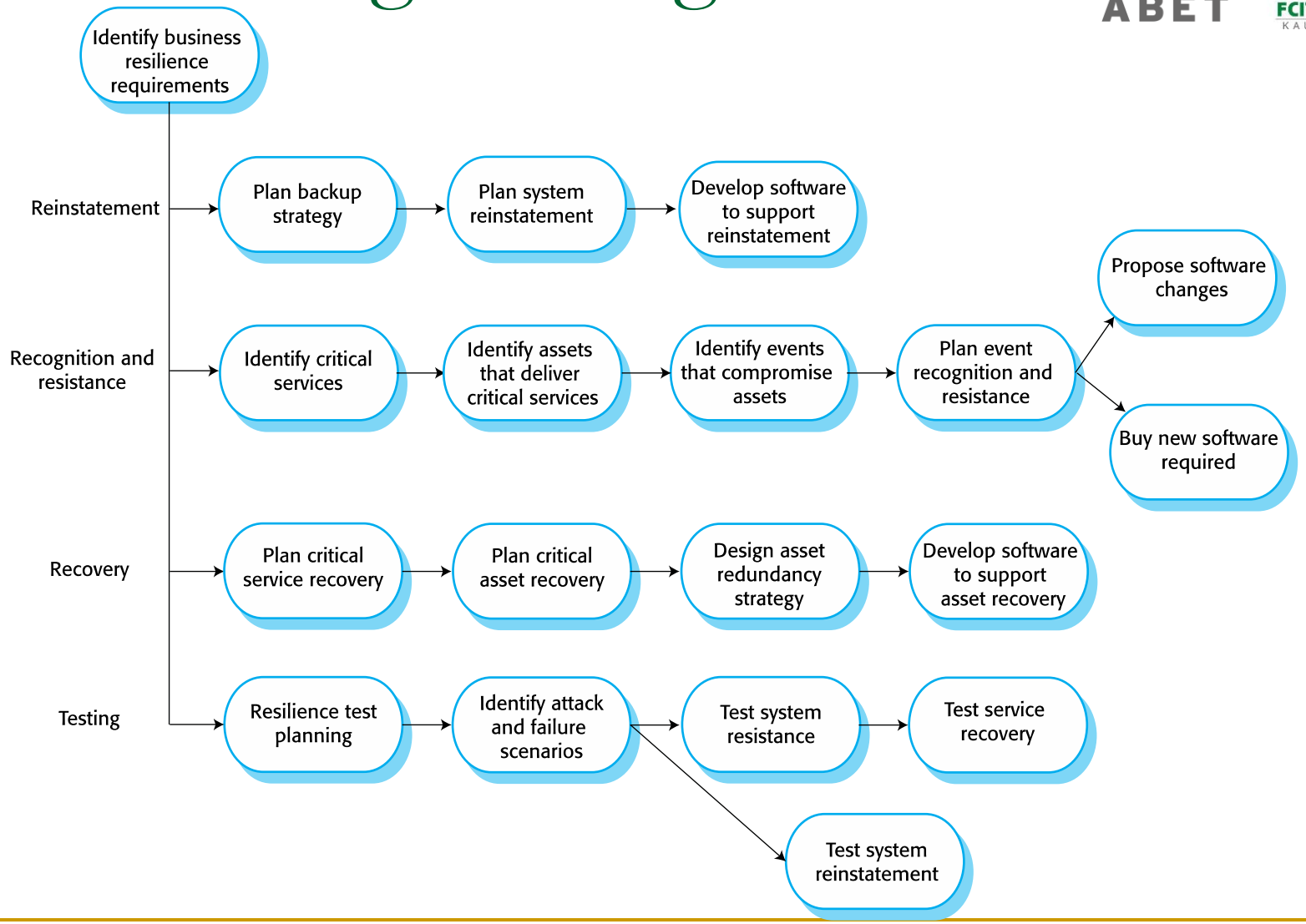
Have a local copy of data

Establish backup server

- Database integrity checker
- Transaction logs
- Database backup

Vulnerabilities -> Threats -> Assets <- Controls

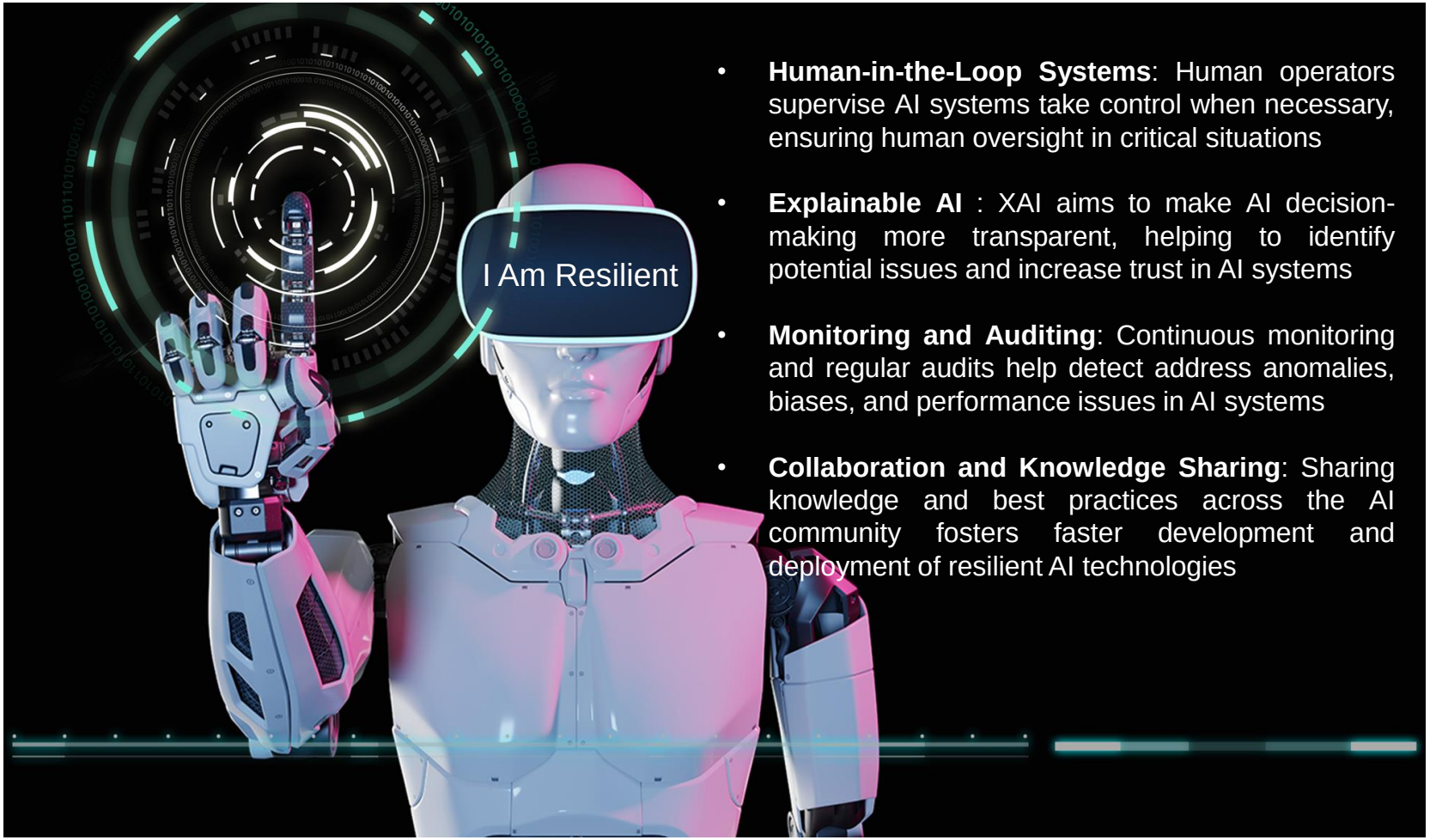
Resilient engineering



R&R strategies

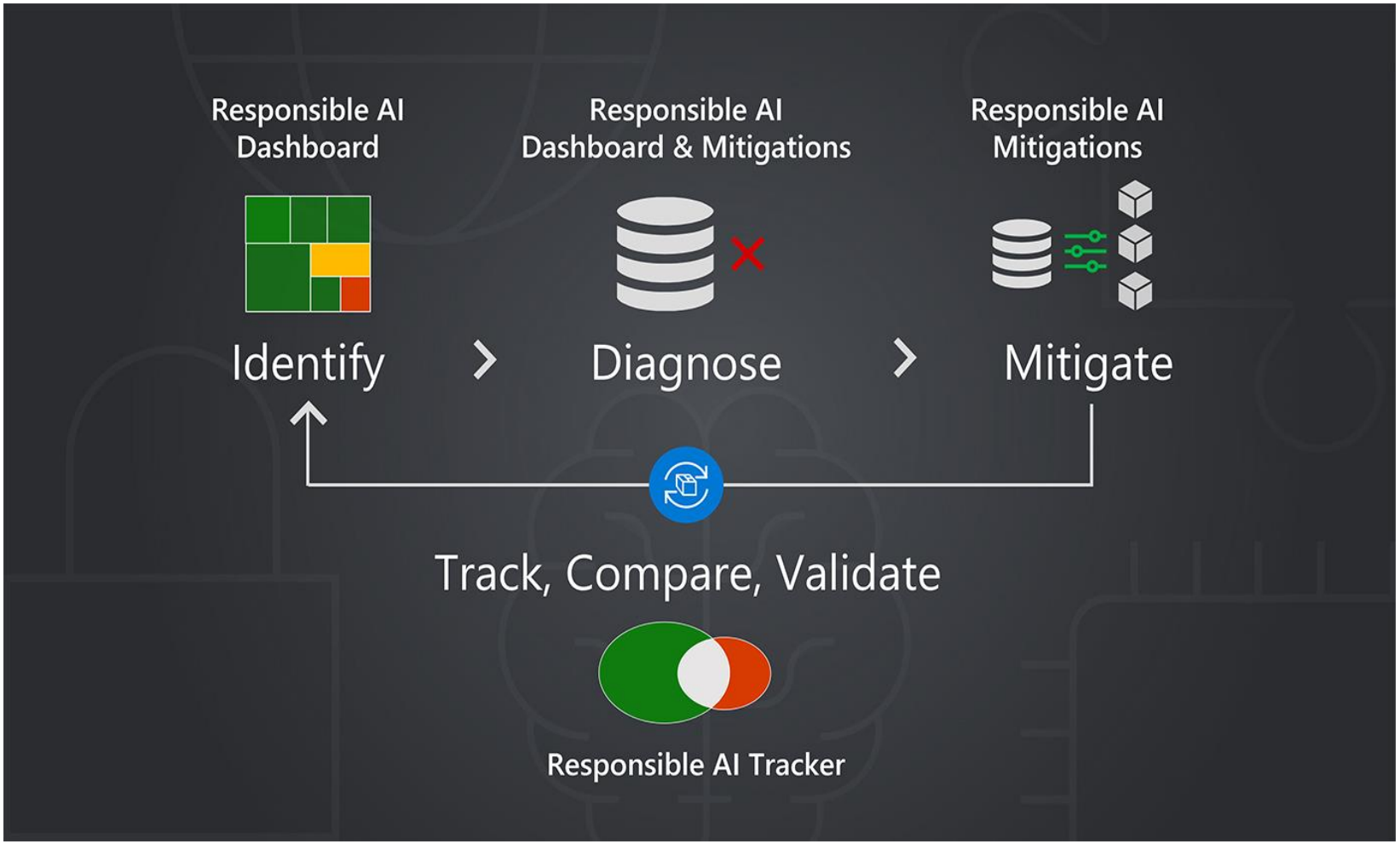
Event	Recognition	Resistance
Server unavailability	1. Watchdog timer on client that times out if no response to client access 2. Text messages from system managers to clinical users	1. Design system architecture to maintain local copies of critical information 2. Provide peer-to-peer search across clients for patient data 3. Provide staff with smart phones that can be used to access the network in the event of server failure 4. Provide backup server
Patient database corruption	1. Record level cryptographic checksums 2. Regular auto-checking of database integrity 3. Reporting system for incorrect information	1. Replayable transaction log to update database backup with recent transactions 2. Maintenance of local copies of patient information and software to restore database from local copies and backups
Malware infection of client computers	1. Reporting system so that computer users can report unusual behaviour. 2. Automated malware checks on startup.	1. Security awareness workshops for all system users 2. Disabling of USB ports on client computers 3. Automated system setup for new clients 4. Support access to system from mobile devices 5. Installation of security software
Unauthorized access to patient information	1. Warning text messages from users about possible intruders 2. Log analysis for unusual activity	1. Multi-level system authentication process 2. Disabling of USB ports on client computers 3. Access logging and real-time log analysis 4. Security awareness workshops for all system users

Resilience engineering in AI era

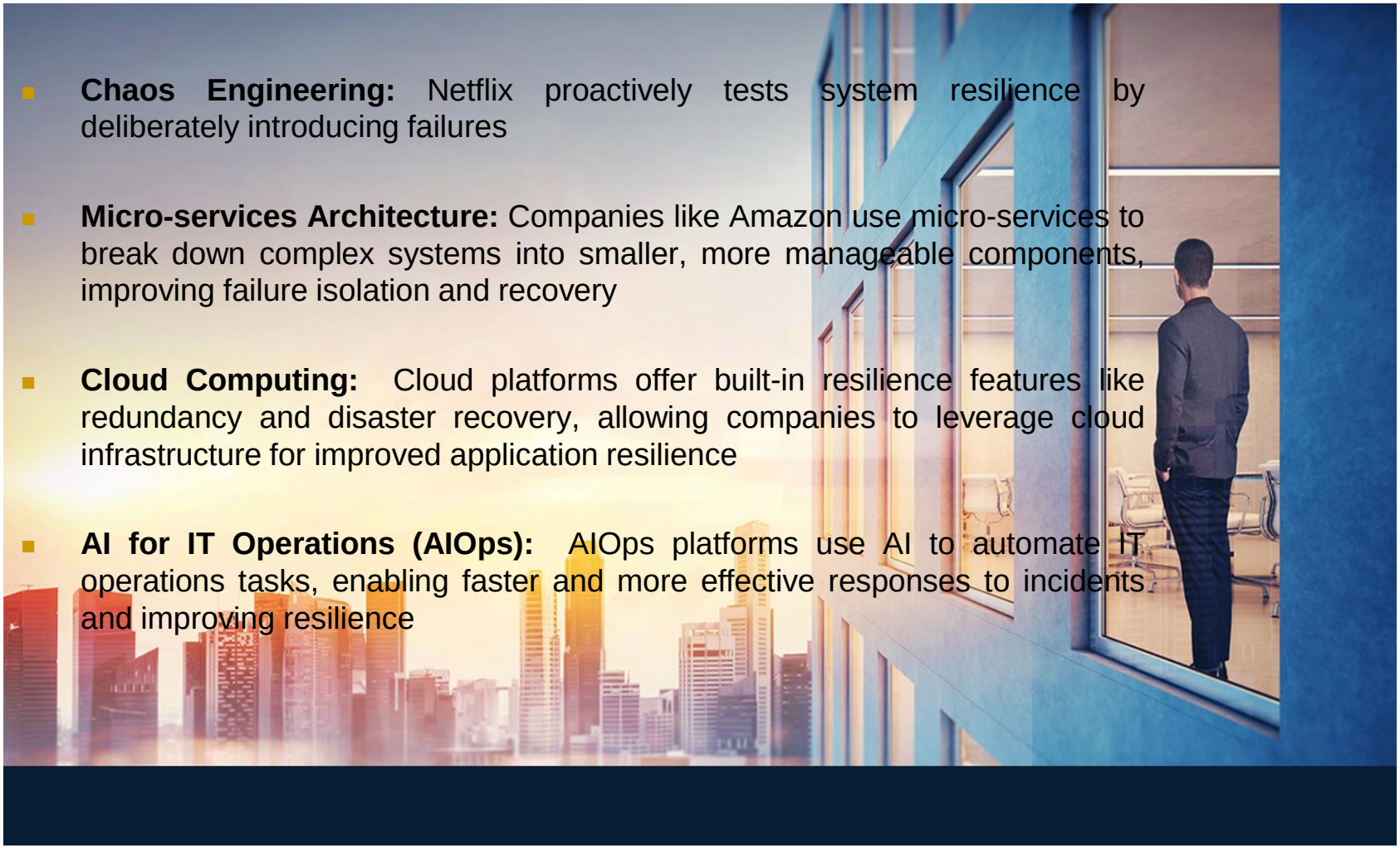


- **Human-in-the-Loop Systems**: Human operators supervise AI systems take control when necessary, ensuring human oversight in critical situations
- **Explainable AI** : XAI aims to make AI decision-making more transparent, helping to identify potential issues and increase trust in AI systems
- **Monitoring and Auditing**: Continuous monitoring and regular audits help detect address anomalies, biases, and performance issues in AI systems
- **Collaboration and Knowledge Sharing**: Sharing knowledge and best practices across the AI community fosters faster development and deployment of resilient AI technologies

Ex; Microsoft resilient AI



Aligning with industry trends



- **Chaos Engineering:** Netflix proactively tests system resilience by deliberately introducing failures
- **Micro-services Architecture:** Companies like Amazon use micro-services to break down complex systems into smaller, more manageable components, improving failure isolation and recovery
- **Cloud Computing:** Cloud platforms offer built-in resilience features like redundancy and disaster recovery, allowing companies to leverage cloud infrastructure for improved application resilience
- **AI for IT Operations (AIOps):** AIOps platforms use AI to automate IT operations tasks, enabling faster and more effective responses to incidents and improving resilience

To master today's lesson

- Assignment 5 is designed to assess your mastery of sixth (CLO): Design systems to support resilience
- Total Marks: 5
- Submission Deadline: 8:00 PM every Saturday. No late submissions accepted
- You can use any LLM (ChatGPT, Claude, etc.), but you must follow the IT department's LLM ethics guidelines
- Collaboration allowed but submit individual work