Chapter 10 – Dependable systems

Topics covered

- ✧ Dependability properties
- ✧ Sociotechnical systems
- ✧ Redundancy and diversity
- ✧ Dependable processes
- ✧ Formal methods and dependability

System dependability

- ✧ The most important system property is the dependability
- ✧ Reflect the user’s degree of trust in that system.
- ✧ Reflect the extent of the user’s confidence that it will operate as users expect.
- ✧ Cover the related attributes: reliability, availability and security.

Importance of dependability

- ✧ System failures may have widespread.
- ✧ Systems that are not dependable may be rejected.
- ✧ The costs of system failure is high if the failure leads to economic losses.
- ✧ Undependable systems may cause information loss.

Causes of failure

✧ Hardware failure

- Design and manufacturing errors.

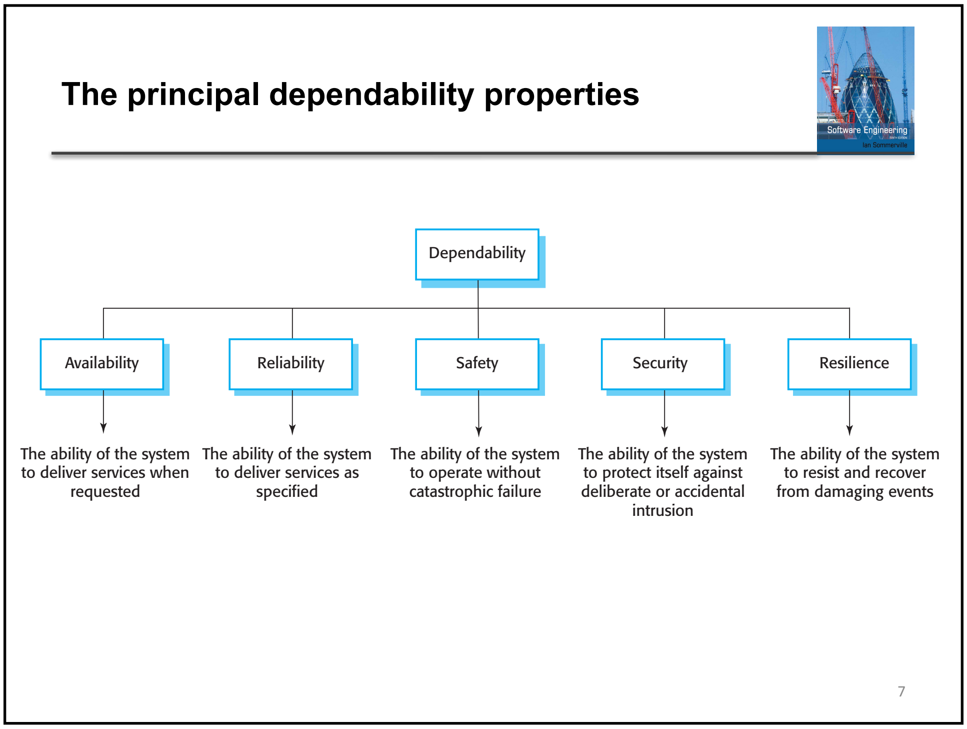
✧ Software failure

- Errors in its implementation.

✧ Operational failure

- Human operators make mistakes.

Dependability properties



The principal dependability properties

Dependability

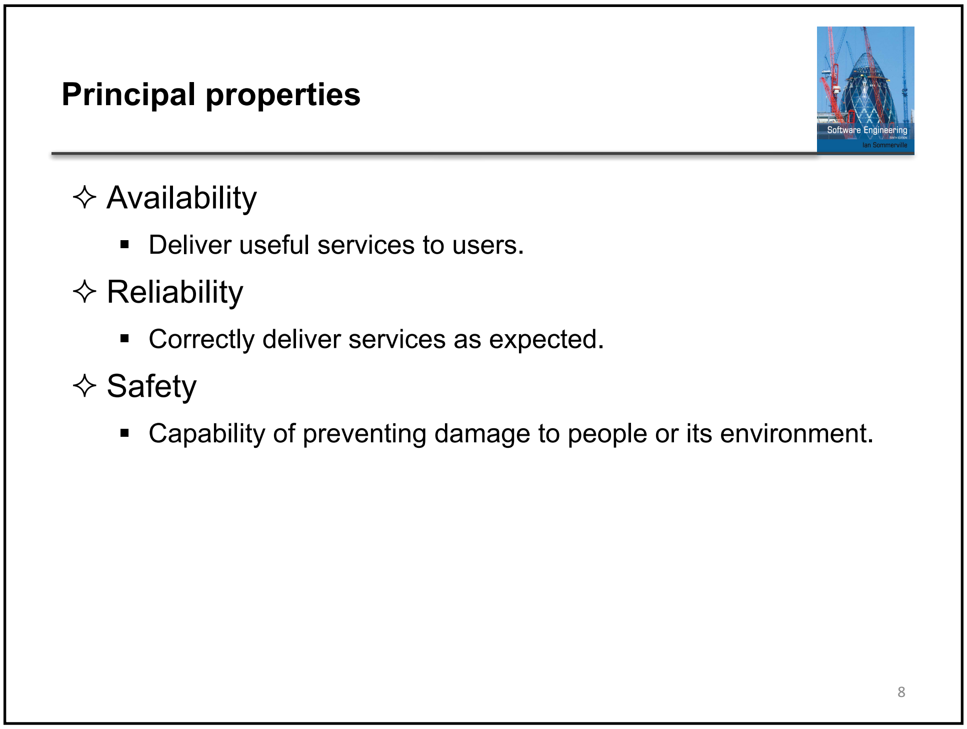
Availability — The ability of the system to deliver services when requested

Reliability — The ability of the system to deliver services as specified

Safety — The ability of the system to operate without catastrophic failure

Security — The ability of the system to protect itself against deliberate or accidental intrusion

Resilience — The ability of the system to resist and recover from damaging events



Principal properties

✧ Availability

- Deliver useful services to users.

✧ Reliability

- Correctly deliver services as expected.

✧ Safety

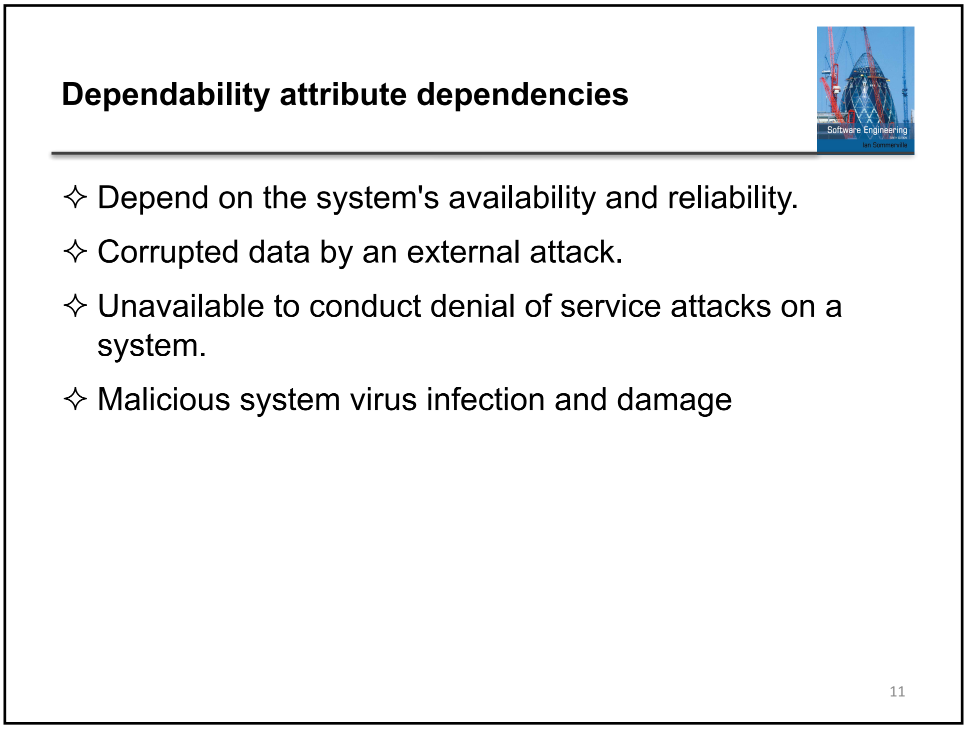
- Capability of preventing damage to people or its environment.

Principal properties

- ✧ Security
  - Capability of resisting accidental or deliberate intrusions.
- ✧ Resilience
  - A judgment of how well a system can maintain the continuity of its critical services.

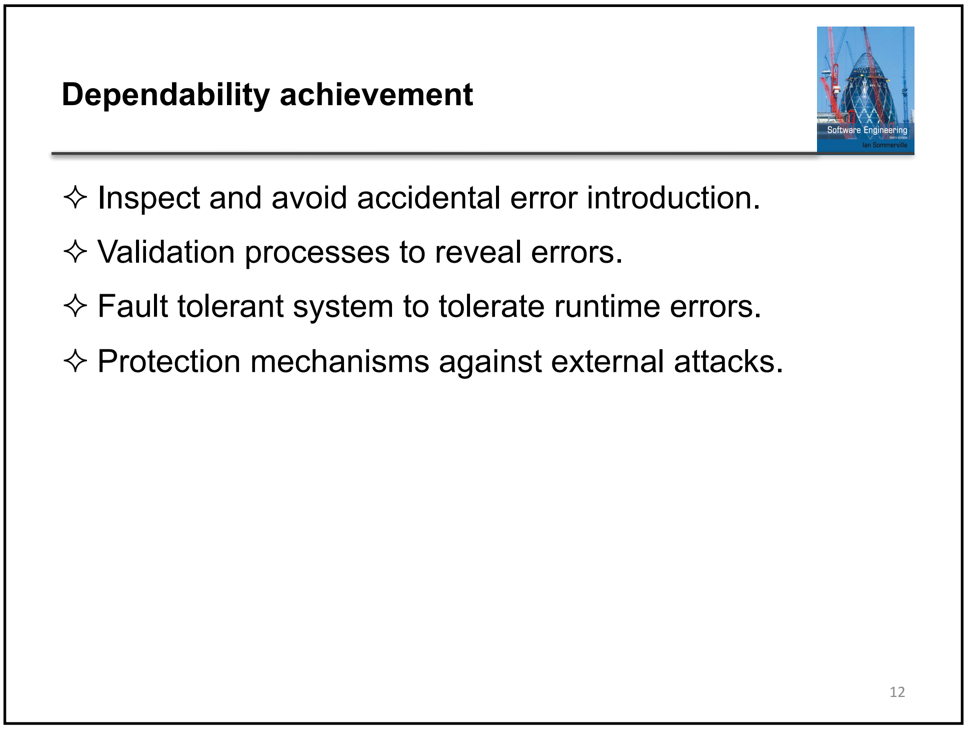
Other dependability properties

- ✧ Repairability
  - Capability of being repaired in the event of a failure
- ✧ Maintainability
  - Capability of being adapted to new requirements
- ✧ Error tolerance
  - Capability to tolerate failures due to user input errors



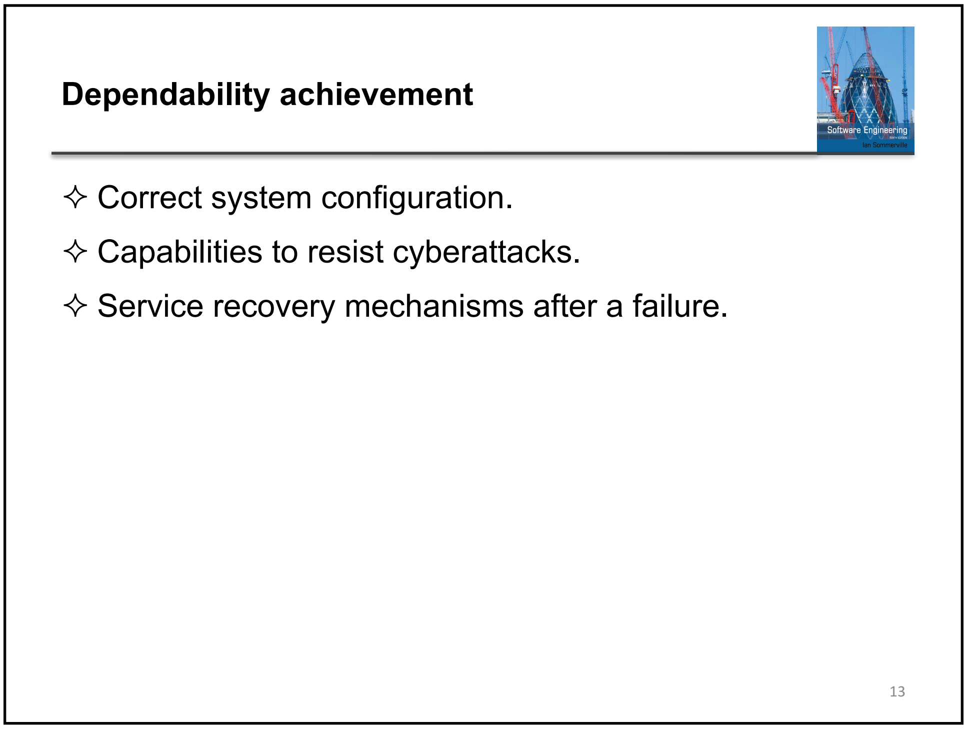
Dependability attribute dependencies

- Depend on the system's availability and reliability.
- Corrupted data by an external attack.
- Unavailable to conduct denial of service attacks on a system.
- Malicious system virus infection and damage



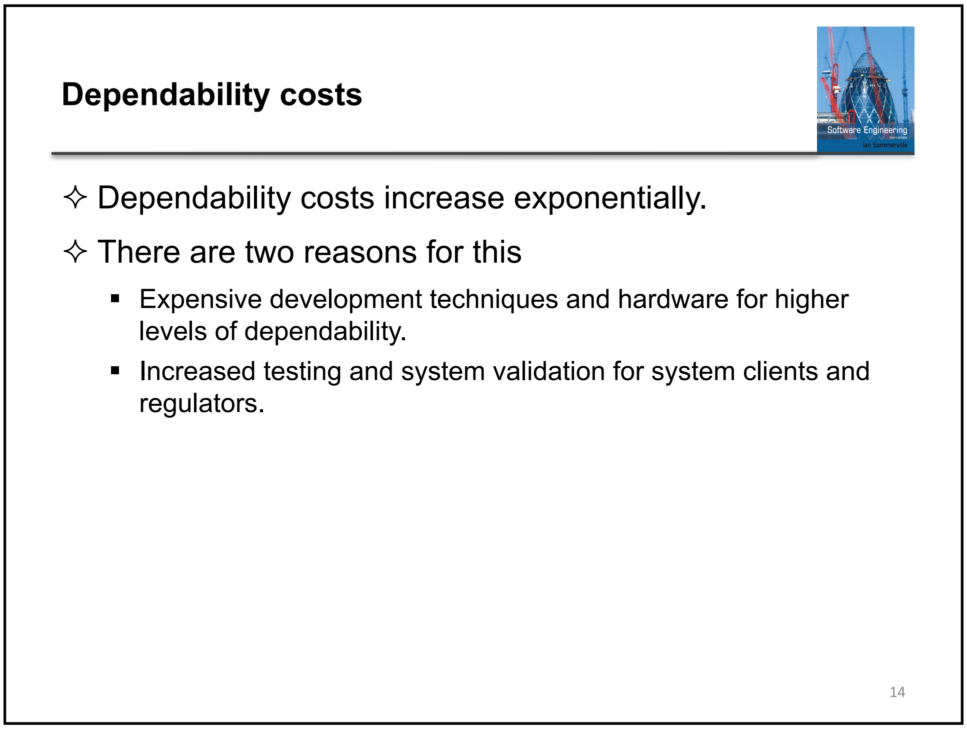
Dependability achievement

- Inspect and avoid accidental error introduction.
- Validation processes to reveal errors.
- Fault tolerant system to tolerate runtime errors.
- Protection mechanisms against external attacks.



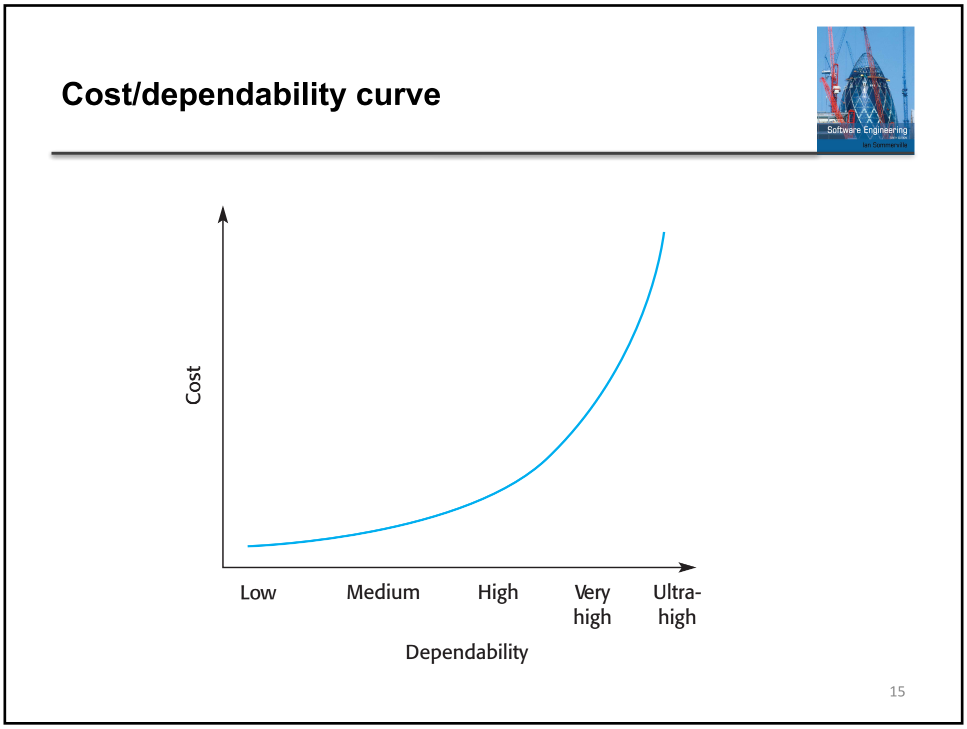
Dependability achievement

- ✧ Correct system configuration.
- ✧ Capabilities to resist cyberattacks.
- ✧ Service recovery mechanisms after a failure.

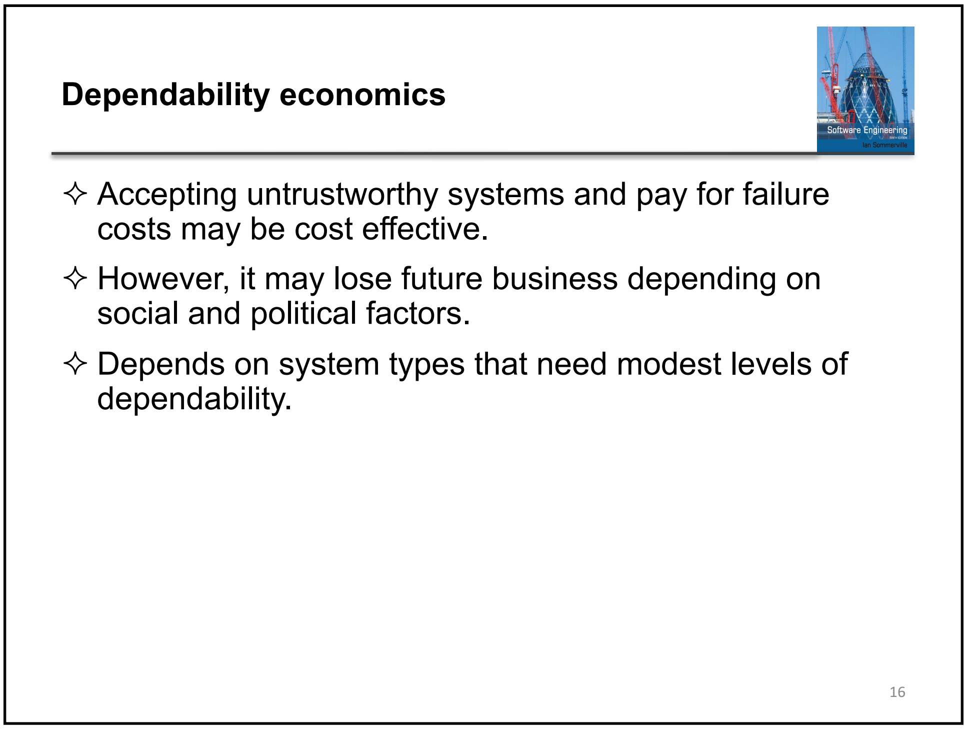


Dependability costs

- ✧ Dependability costs increase exponentially.
- ✧ There are two reasons for this
  - Expensive development techniques and hardware for higher levels of dependability.
  - Increased testing and system validation for system clients and regulators.

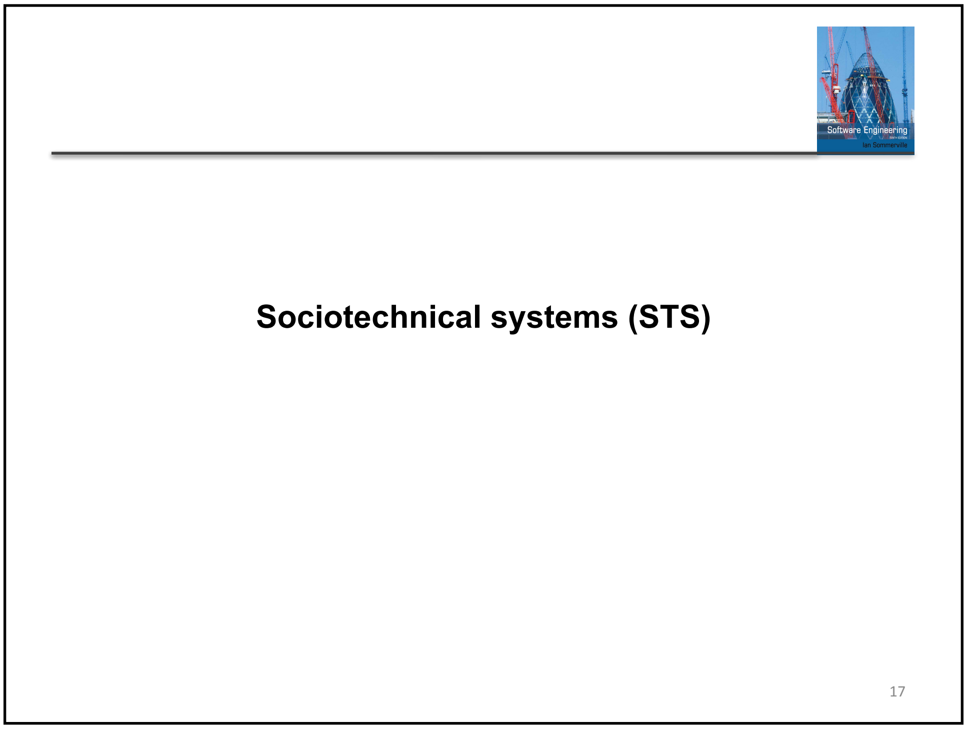


Cost/dependability curve

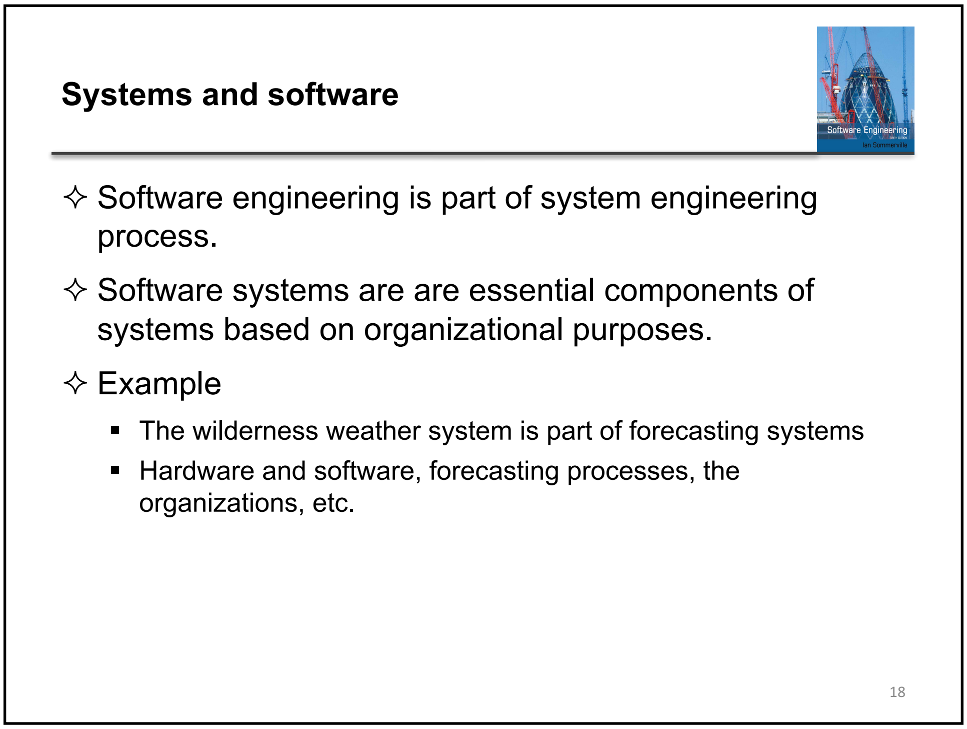


Dependability economics

- ✧ Accepting untrustworthy systems and pay for failure costs may be cost effective.
- ✧ However, it may lose future business depending on social and political factors.
- ✧ Depends on system types that need modest levels of dependability.



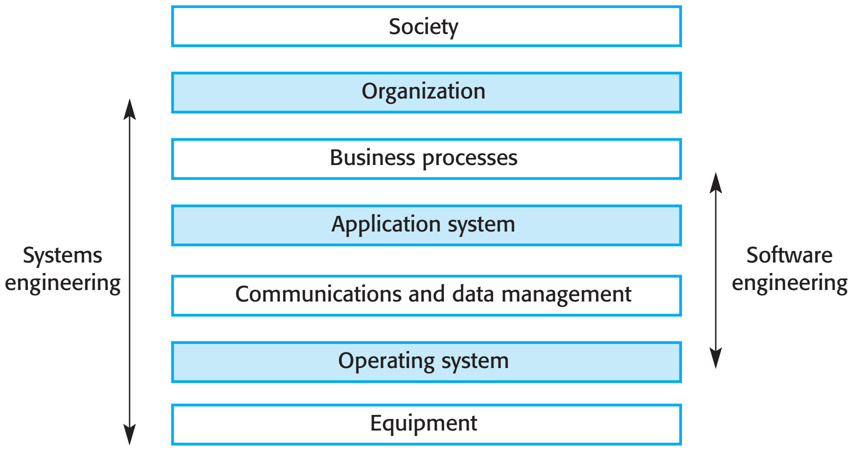
Sociotechnical systems (STS)



Systems and software

- ✧ Software engineering is part of system engineering process.
- ✧ Software systems are are essential components of systems based on organizational purposes.
- ✧ Example
  - The wilderness weather system is part of forecasting systems
  - Hardware and software, forecasting processes, the organizations, etc.

The sociotechnical systems (STS) stack



Society

Organization

Business processes

Application system

Communications and data management

Operating system

Equipment

Systems engineering

Software engineering

Layers in the STS stack

- ✧ Equipment
  - Hardware devices, including embedded systems
- ✧ Operating system
  - Common facilities for higher level applications.
- ✧ Communications and data management
  - Access to remote systems and databases.
- ✧ Application systems
  - Functionalities for specific requirements.

Layers in the STS stack

✧ Business processes

- Processes involving people and systems

✧ Organizations

- Business activities for system operations

✧ Society

- Laws, regulation and culture

Holistic system design

✧ Interactions and dependencies between system layers

- Example: regulation changes causes changes in applications.

✧ For dependability, a systems perspective is essential

- Software failures within the enclosing layers.
- Failures in adjacent layers affects software systems.

Regulation and compliance

✧ The general model of economic organization

- Universal in the world.
- Offer goods and services and make a profit.

✧ Ensure the safety of their citizens

- Follow standards to ensure that products are safe and secure.

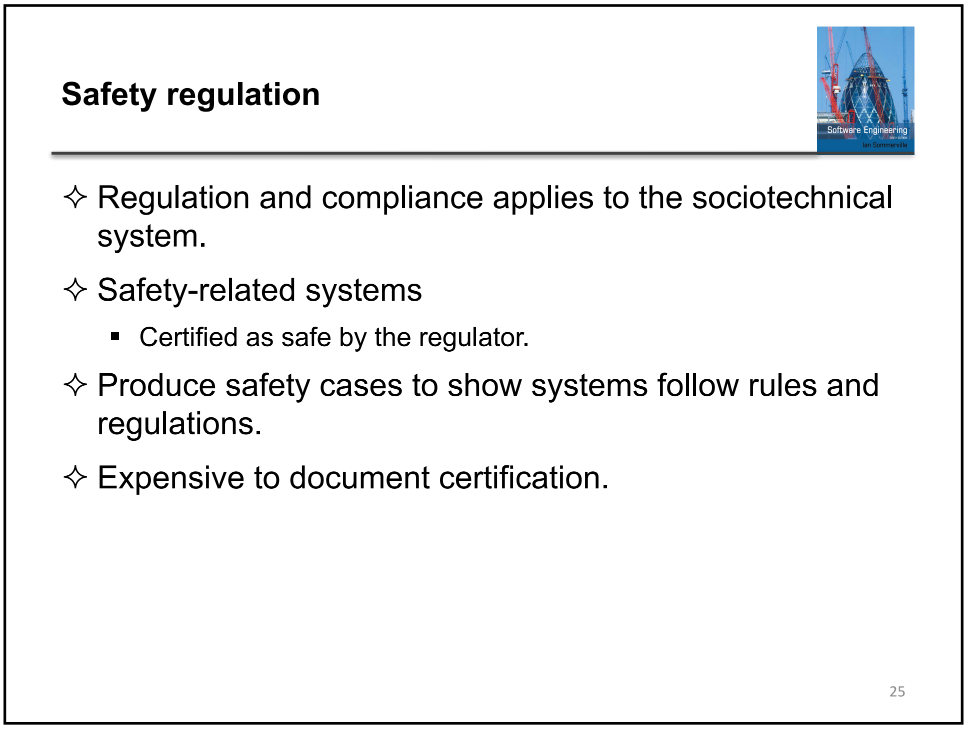
Regulated systems

✧ Critical systems are regulated systems

- Approved by an external regulator.
- E.g., nuclear systems and air traffic control systems

✧ A safety and dependability case

- Approved by the regulator.
- Create the evidence for systems' dependability, safety and security.



Safety regulation

- Regulation and compliance applies to the sociotechnical system.
- Safety-related systems
  - Certified as safe by the regulator.
- Produce safety cases to show systems follow rules and regulations.
- Expensive to document certification.