Iran University of Science and Technology
Computer engineering Department

Basic Concepts and Taxonomy of Dependable and Secure Computing

Alireza Saberi
Instructor:
Dr. Abdollahi Azgomi

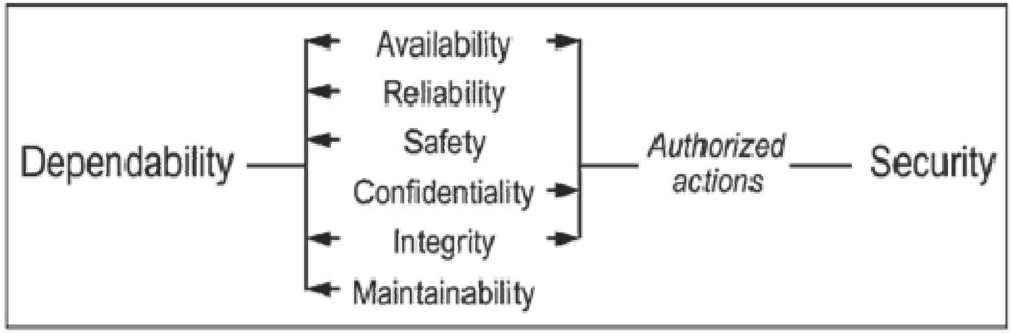
May, 2008

Outline

- ✓Dependability and Security Definition
- ✓The Attributes of Dependability and Security
- ✓The Means to Attain Dependability and Security
    - ➢Fault Prevention
    - ➢Fault Tolerance
    - ➢Fault Removal
    - ➢Fault Forecasting
- ✓Conclusion

Dependability and Security Definition

- ✓ **The origin definition:** the ability to deliver service that can justifiably be trusted.
- ✓ **The alternate definition:** the ability of a system to avoid service failures that are more frequent or more severe than is acceptable.
- ✓ Security has not been characterized as a single attribute of dependability, it is combination of ***confidentiality***, ***integrity*** and ***availability***.



Relationship between dependability and security.

Dependence and Trust

- ✓ The dependence of system A on system B represents the extent to which System A's dependability is (or would be) affected by that of System B.
- ✓ Trust is accepted dependence.
- ✓ Total dependence: any failure of B would cause A to fail
- ✓ Complete independence: B cannot cause A to fail

Outline

- ✓ **Dependability and Security Definition**
- ✓ The Attributes of Dependability and Security
- ✓ The Means to Attain Dependability and Security
  - ➢ Fault Prevention
  - ➢ Fault Tolerance
  - ➢ Fault Removal
  - ➢ Fault Forecasting
- ✓ Conclusion

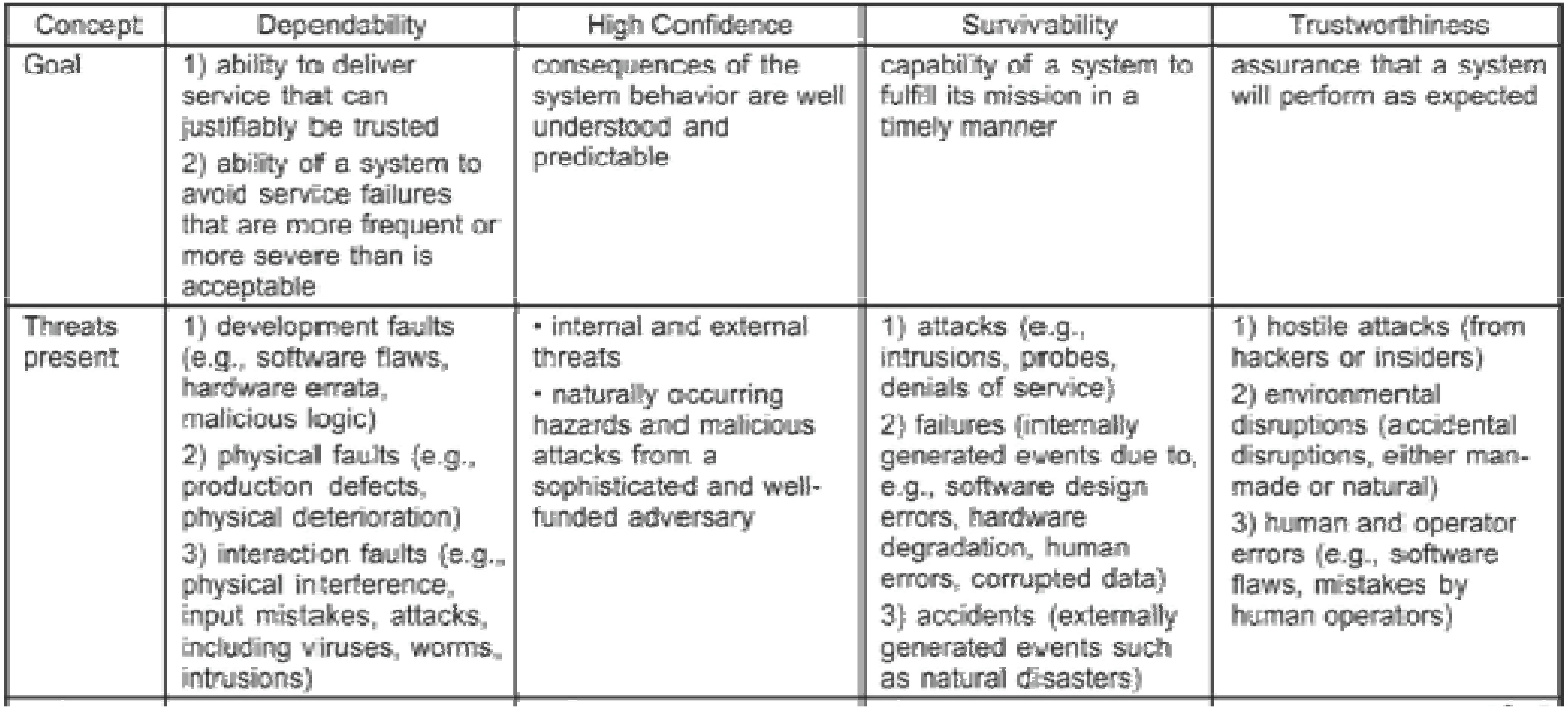
The Attributes of Dependability and Security

- ✓ **Primary attributes**
  - ➢ Availability, integrity and maintainability are generally required, although to a varying degree depending on the application
  - ➢ Reliability, safety and confidentiality may or may not be required according to the application

The Attributes of Dependability and Security (Cont.)

- ✓ **Secondary attributes:** The notion of secondary attributes is especially relevant for security.
  - ➢ **Robustness**: dependability with respect to external faults.
  - ➢ **Accountability**: availability and integrity of the identity of the person who performed an operation.
  - ➢ **Authenticity**: integrity of a message content and origin, and possibly of some other information, such as the time of emission.
  - ➢ **Non-repudiability**: availability and integrity of the identity of the sender of a message or of the receiver.

Dependability, High Confidence Survivability, Trustworthiness



Concept	Dependability	High Confidence	Survivability	Trustworthiness
Goal	1) ability to deliver service that can justifiably be trusted 2) ability of a system to avoid service failures that are more frequent or more severe than is acceptable	consequences of the system behavior are well understood and predictable	capability of a system to fulfill its mission in a timely manner	assurance that a system will perform as expected
Threats present	1) development faults (e.g., software flaws, hardware errata, malicious logic) 2) physical faults (e.g., production defects, physical deterioration) 3) interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)	• internal and external threats • naturally occurring hazards and malicious attacks from a sophisticated and well-funded adversary	1) attacks (e.g., intrusions, probes, denials of service) 2) failures (internally generated events due to, e.g., software design errors, hardware degradation, human errors, corrupted data) 3) accidents (externally generated events such as natural disasters)	1) hostile attacks (from hackers or insiders) 2) environmental disruptions (accidental disruptions, either man-made or natural) 3) human and operator errors (e.g., software flaws, mistakes by human operators)

✓A side by side comparison leads to the conclusion that all four concepts are essentially equivalent in their goals and address similar threats.

Outline

- ✓ **Dependability and Security Definition**
- ✓ **The Attributes of Dependability and Security**
- ✓ The Means to Attain Dependability and Security
  - ➢ Fault Prevention
  - ➢ Fault Tolerance
  - ➢ Fault Removal
  - ➢ Fault Forecasting
- ✓ Conclusion

The Means to Attain Dependability and Security

- ✓Fault Prevention
- ✓Fault Tolerance
- ✓Fault Removal
- ✓Fault Forecasting

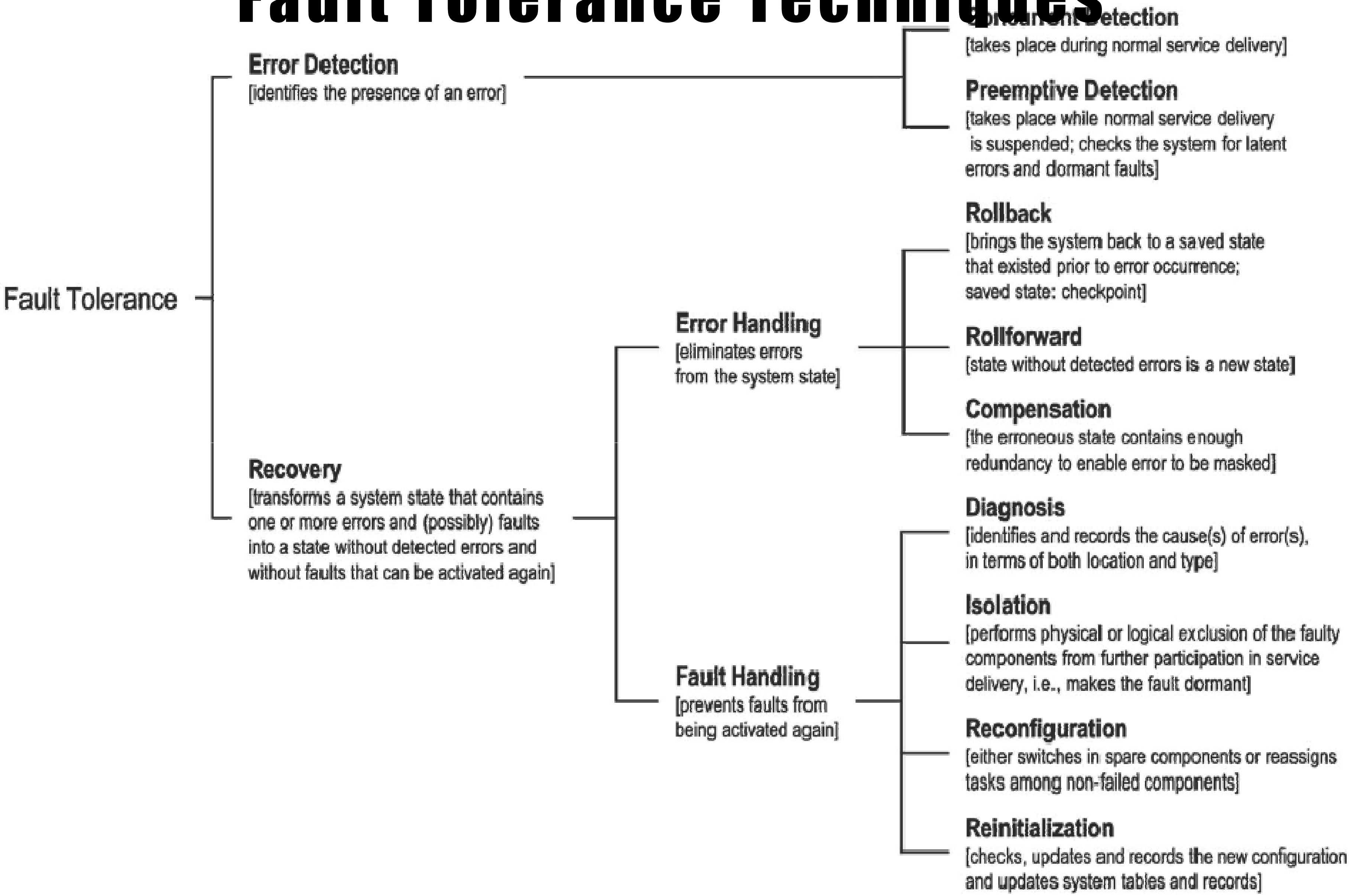
Fault Prevention

- ✓ Fault prevention is part of general engineering.
- ✓ Prevention of development faults is an obvious aim for development methodologies.
- ✓ Elimination of the causes of the faults via process modifications.

Fault Tolerance

- ✓ **Fault tolerance**, which is aimed at failure avoidance, is carried out **via error detection** and **system recovery**.
- ✓ Fault handling is followed by corrective maintenance, aimed at removing faults that were isolated by fault handling.
- ✓ Rollback and Rollforward are invoked on demand, after error detection has taken place.
- ✓ Error handling on demand followed by fault handling together form system recovery.

Fault Tolerance Techniques



Fault Tolerance

Error Detection
[identifies the presence of an error]

Concurrent Detection
[takes place during normal service delivery]

Preemptive Detection
[takes place while normal service delivery is suspended; checks the system for latent errors and dormant faults]

Recovery
[transforms a system state that contains one or more errors and (possibly) faults into a state without detected errors and without faults that can be activated again]

Error Handling
[eliminates errors from the system state]

Rollback
[brings the system back to a saved state that existed prior to error occurrence;
saved state: checkpoint]

Rollforward
[state without detected errors is a new state]

Compensation
[the erroneous state contains enough redundancy to enable error to be masked]

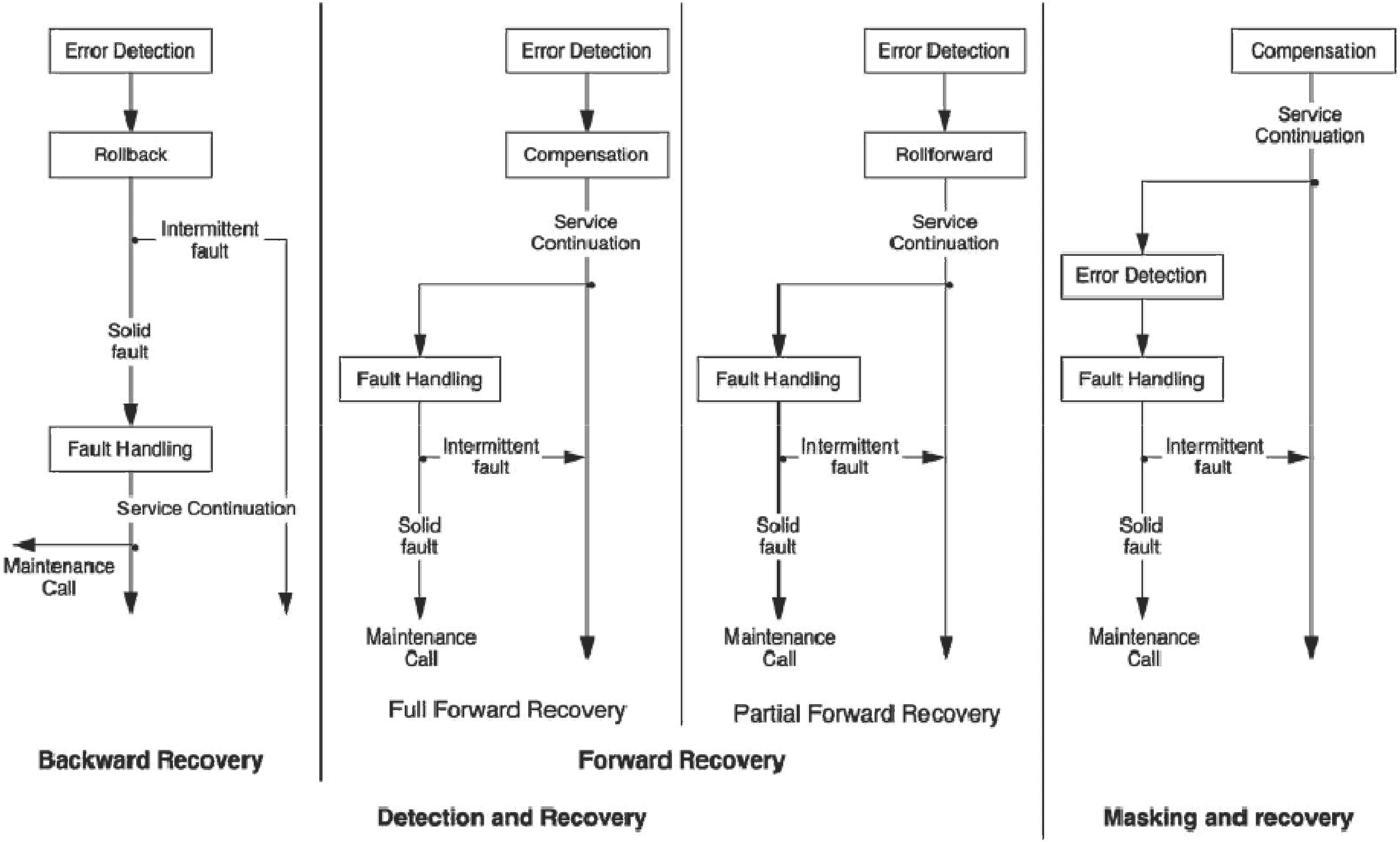
Fault Handling
[prevents faults from being activated again]

Diagnosis
[identifies and records the cause(s) of error(s), in terms of both location and type]

Isolation
[performs physical or logical exclusion of the faulty components from further participation in service delivery, i.e., makes the fault dormant]

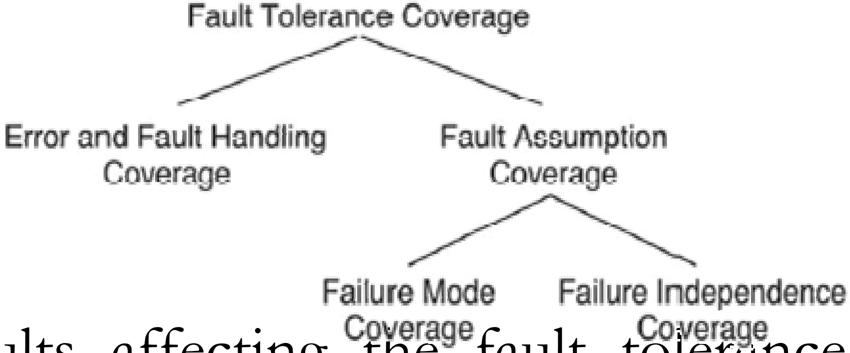
Reconfiguration
[either switches in spare components or reassigns tasks among non-failed components]

Reinitialization
[checks, updates and records the new configuration and updates system tables and records]


Error Detection
Rollback
Intermittent fault
Solid fault
Fault Handling
Service Continuation
Maintenance Call
Backward Recovery
Error Detection
Compensation
Service Continuation
Fault Handling
Intermittent fault
Solid fault
Maintenance Call
Full Forward Recovery
Error Detection
Rollforward
Service Continuation
Fault Handling
Intermittent fault
Solid fault
Maintenance Call
Partial Forward Recovery
Forward Recovery
Detection and Recovery
Compensation
Service Continuation
Error Detection
Fault Handling
Intermittent fault
Solid fault
Maintenance Call
Masking and recovery

Fault Tolerance Coverage

- ✓ The measure of effectiveness of any given fault tolerance technique is called its **coverage.**



Fault Tolerance Coverage

Error and Fault Handling Coverage

Fault Assumption Coverage

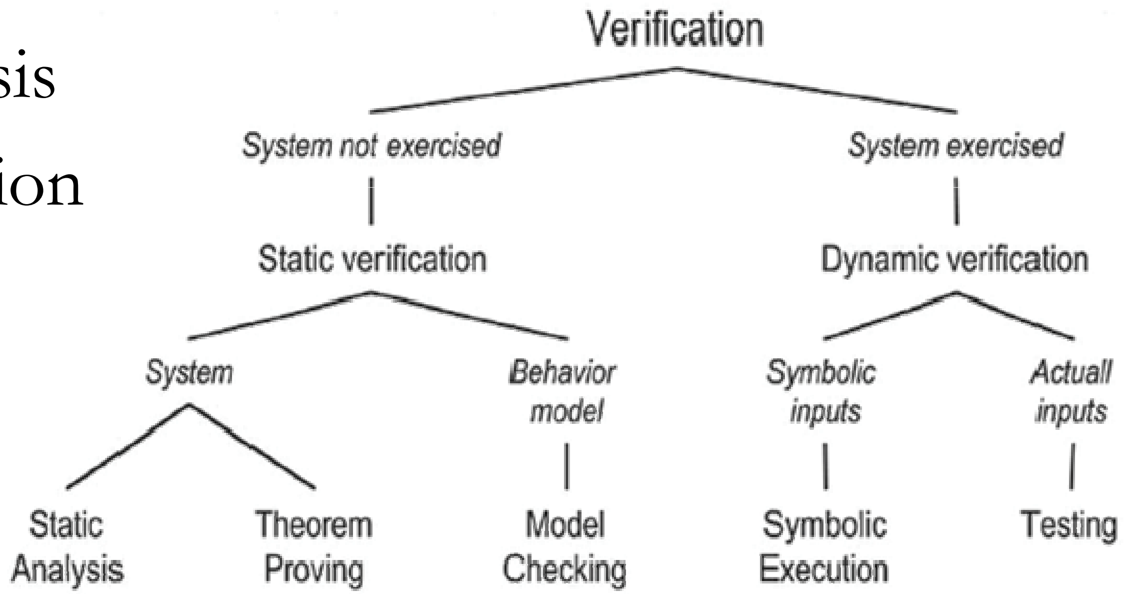
Failure Mode Coverage

Failure Independence Coverage

- ✓ Development faults affecting the fault tolerance mechanisms with respect to the fault assumptions stated during the development, the consequence of which is a lack of error and fault handling coverage.
- ✓ Fault assumptions that differ from the faults really occurring in operation.

Fault Removal

- ✓ Fault Removal During Development
  - ➢Step 1 : Verification
  - ➢Step 2 : Diagnosis
  - ➢Step 3 : Correction



Fault Removal During Use

- ✓ **Corrective** or **preventive** maintenance.
- ✓ Corrective: remove faults that have produced one or more errors and have been reported
- ✓ Preventive: uncovering and removing faults before they might cause errors

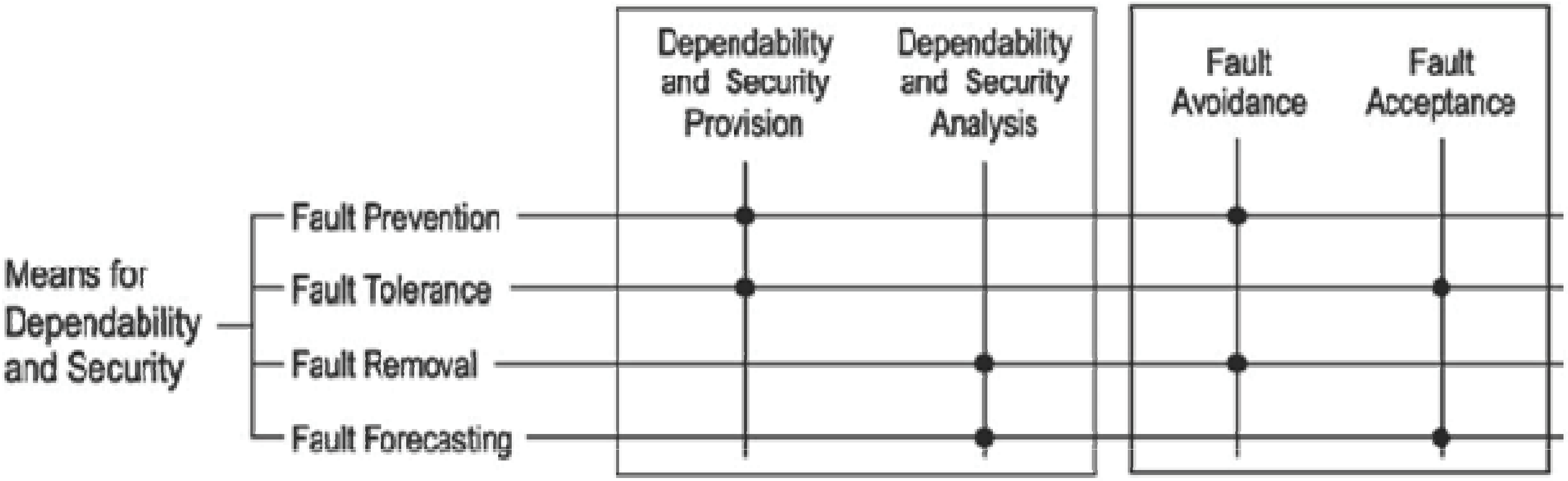
Fault Forecasting

- ✓ An **evaluation** of the system behavior with respect to fault occurrence or activation.
- ✓ Evaluation has two aspects:
  - ➢ Qualitative or ordinal evaluation
    - Identify, classify and rank the failure modes, e.g. failure mode and effect analysis
  - ➢ Quantitative or probabilistic evaluation
    - evaluate in terms of probabilities the extent to which some of the attributes are satisfied, e.g. Markov chains and stochastic, Petri nets

Probabilistic FAULT-FORECASTING

- ✓ Two main approaches
  - ➢ Modeling
  - ➢ Testing
- ✓ Modeling is composed of two phases:
  - ➢ Construction of a model
  - ➢ Processing the model to obtain the expressions and the values of the dependability measures of the system

Relation Between The Means



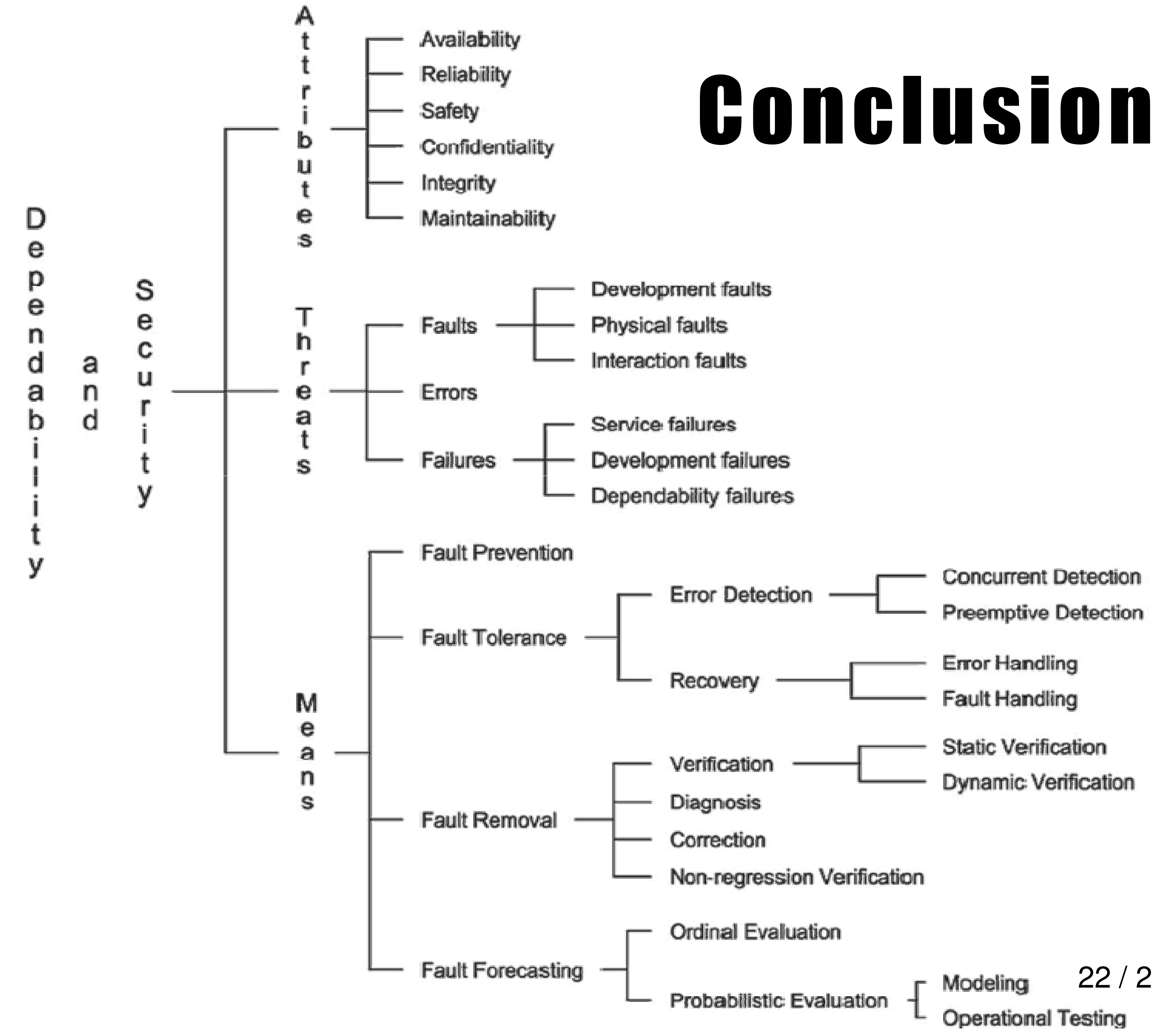
Means for Dependability and Security	Dependability and Security Provision	Dependability and Security Analysis	Fault Avoidance	Fault Acceptance
Fault Prevention	●		●	
Fault Tolerance	●			●
Fault Removal		●	●	
Fault Forecasting		●		●

- ✓ **Fault avoidance**: How to aim for fault-free systems.
- ✓ **Fault acceptance**: How to live with systems that are subject to faults.
- ✓ **Dependability and security analysis**: Reaching confidence in the ability to deliver a service that can be trusted.
- ✓ **Dependability and security provision**: Providing the ability to deliver a service that can be trusted.

Outline

- ✓ **Dependability and Security Definition**
- ✓ **The Attributes of Dependability and Security**
- ✓ **The Means to Attain Dependability and Security**
  - ➢ **Fault Prevention**
  - ➢ **Fault Tolerance**
  - ➢ **Fault Removal**
  - ➢ **Fault Forecasting**
- ✓ Conclusion

Conclusion



Dependability and Security
Attributes
Availability
Reliability
Safety
Confidentiality
Integrity
Maintainability
Threats
Faults
Development faults
Physical faults
Interaction faults
Errors
Failures
Service failures
Development failures
Dependability failures
Means
Fault Prevention
Fault Tolerance
Error Detection
Concurrent Detection
Preemptive Detection
Recovery
Error Handling
Fault Handling
Fault Removal
Verification
Static Verification
Dynamic Verification
Diagnosis
Correction
Non-regression Verification
Fault Forecasting
Ordinal Evaluation
Probabilistic Evaluation
Modeling
Operational Testing

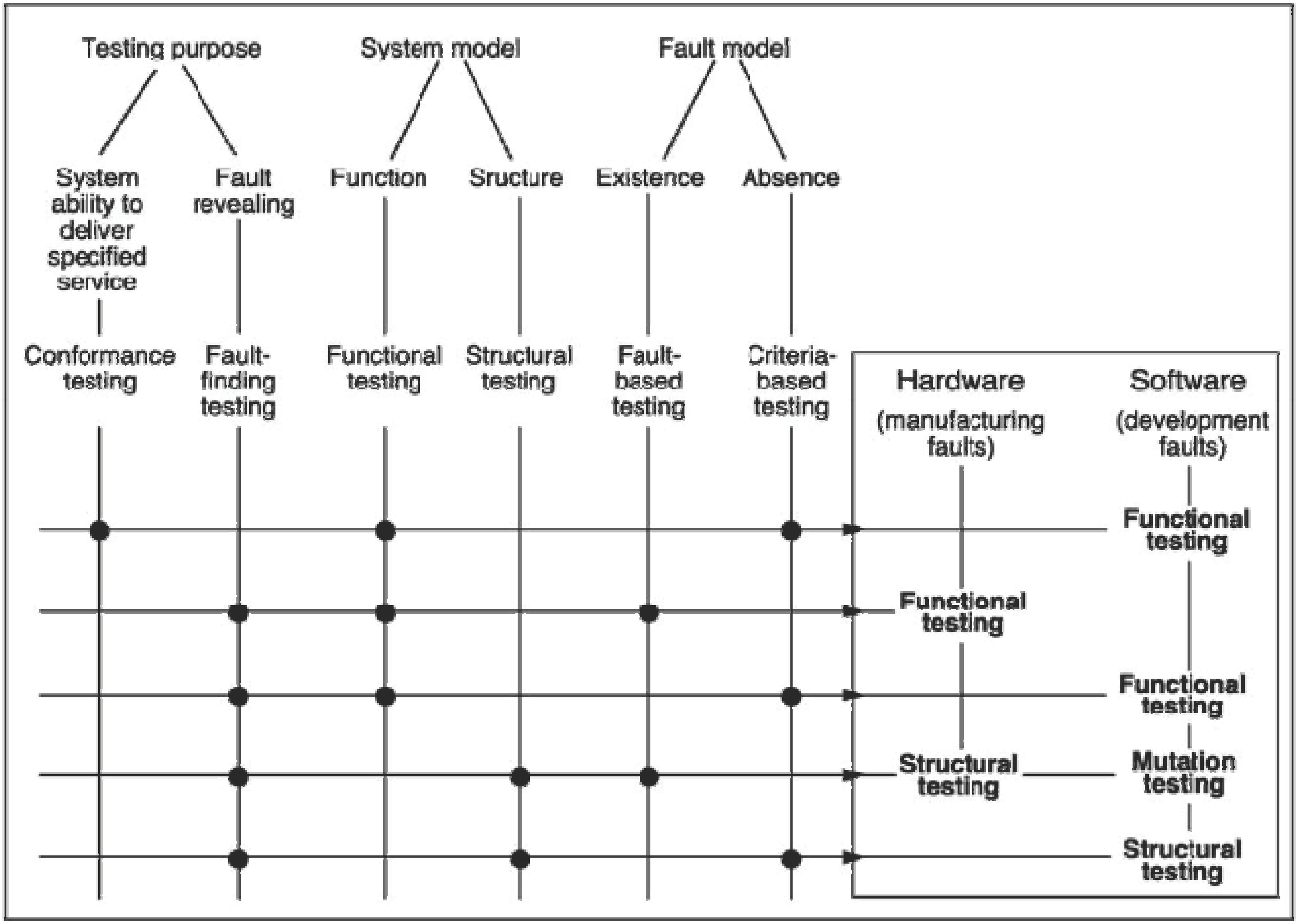
?
R
P

References

- A. Avizienis, J.C. Laprie, B. Randell and C. Landwehr, *"Basic Concepts and Taxonomy of Dependable and Secure Computing,"* IEEE Trans. on Dependable and Secure Computing 1(1) (2004) 11-33

Thanks for your attendance

Testing approaches


Testing purpose
System model
Fault model
System ability to deliver specified service
Fault revealing
Function
Sructure
Existence
Absence
Conformance testing
Fault-finding testing
Functional testing
Structural testing
Fault-based testing
Criteria-based testing
Hardware (manufacturing faults)
Software (development faults)
Functional testing
Functional testing
Functional testing
Structural testing
Mutation testing
Structural testing