Dependability vs Survivability vs Trustworthiness

Jean-Claude Laprie

Based on
A. Avizienis (UCLA), J.C. Laprie, B. Randell (Univ. Of Newcastle upon Tyne): *Fundamental Concepts* of *Dependability*

42 nd 10.4 meeting — Hilton Head Island
Workshop on Dependability and Survivability

Concept	Dependability	Survivability	Trustworthiness
Goal	1) ability of a system to deliver service that can justifiably be trusted 2) ability of a system to avoid failures that are more frequent or more severe than is acceptable to the user(s)	capability of a system to fulfill its mission in a timely manner	assurance that a system will perform as expected
Threats present	1) design faults (e.g., software flaws, hardware errata, malicious logics) 2) physical faults (e.g., production defects, physical deterioration) 3) interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)	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 human-made or natural) 3) human and operator errors (e.g., software flaws, mistakes by human operators)
Reference	«Fundamental concepts of dependability»[1]	«Survivable network systems»[2]	«Trust in cyberspace»[3]

1 A. Avizienis, J.C. Laprie, B. Randell, "Fundamental concepts of dependability", March 2001.

2 R.J. Ellison, D.A. Fischer, R.C. Linger, H.F. Lipson, T. Longstaff, N.R. Mead, "Survivable network systems: an emerging discipline", Technical Report CMU/SEI-97-TR-013, November 1997, revised May 1999.

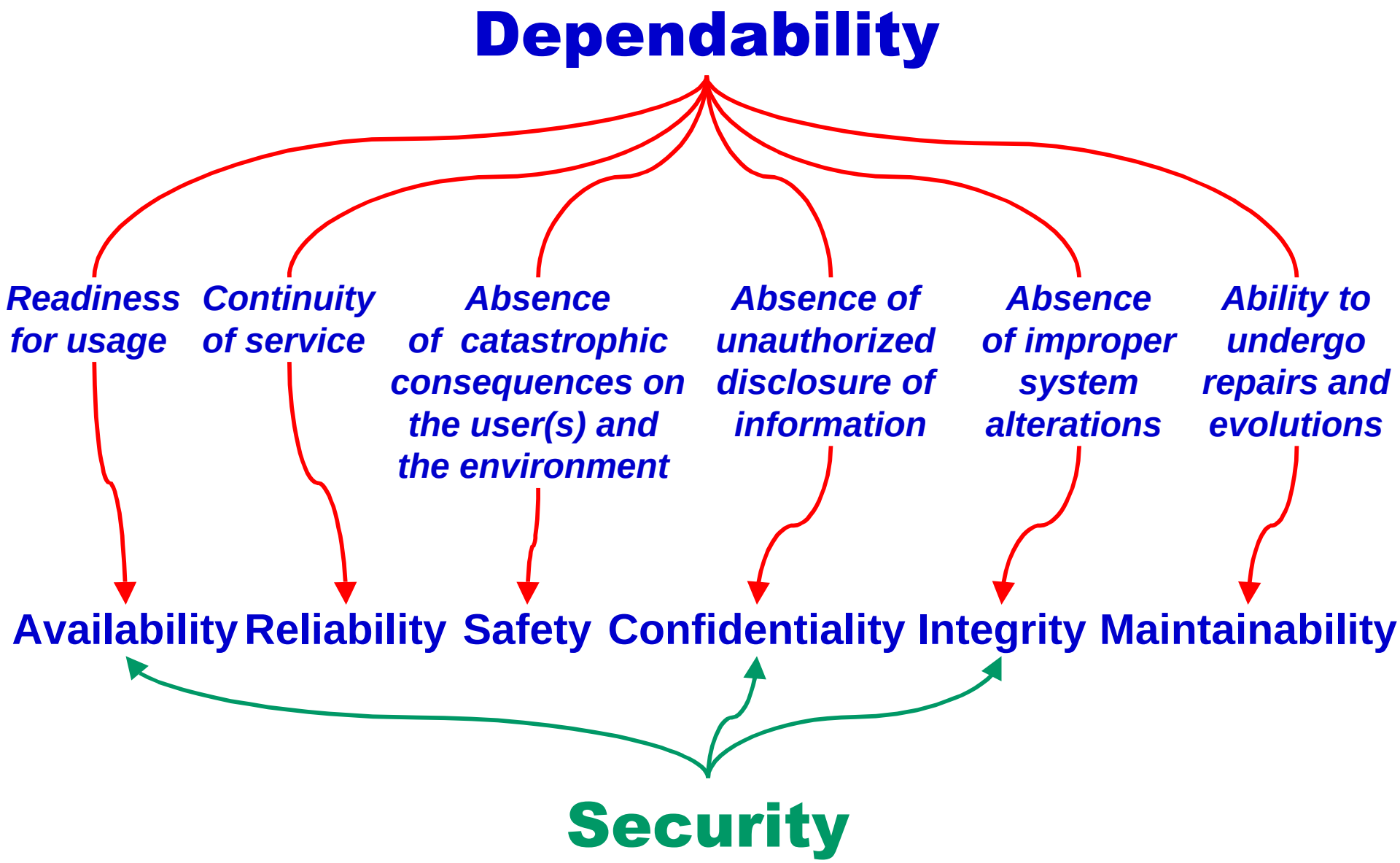
3 F. Schneider, ed., *Trust in Cyberspace*, National Academy Press, 1999.

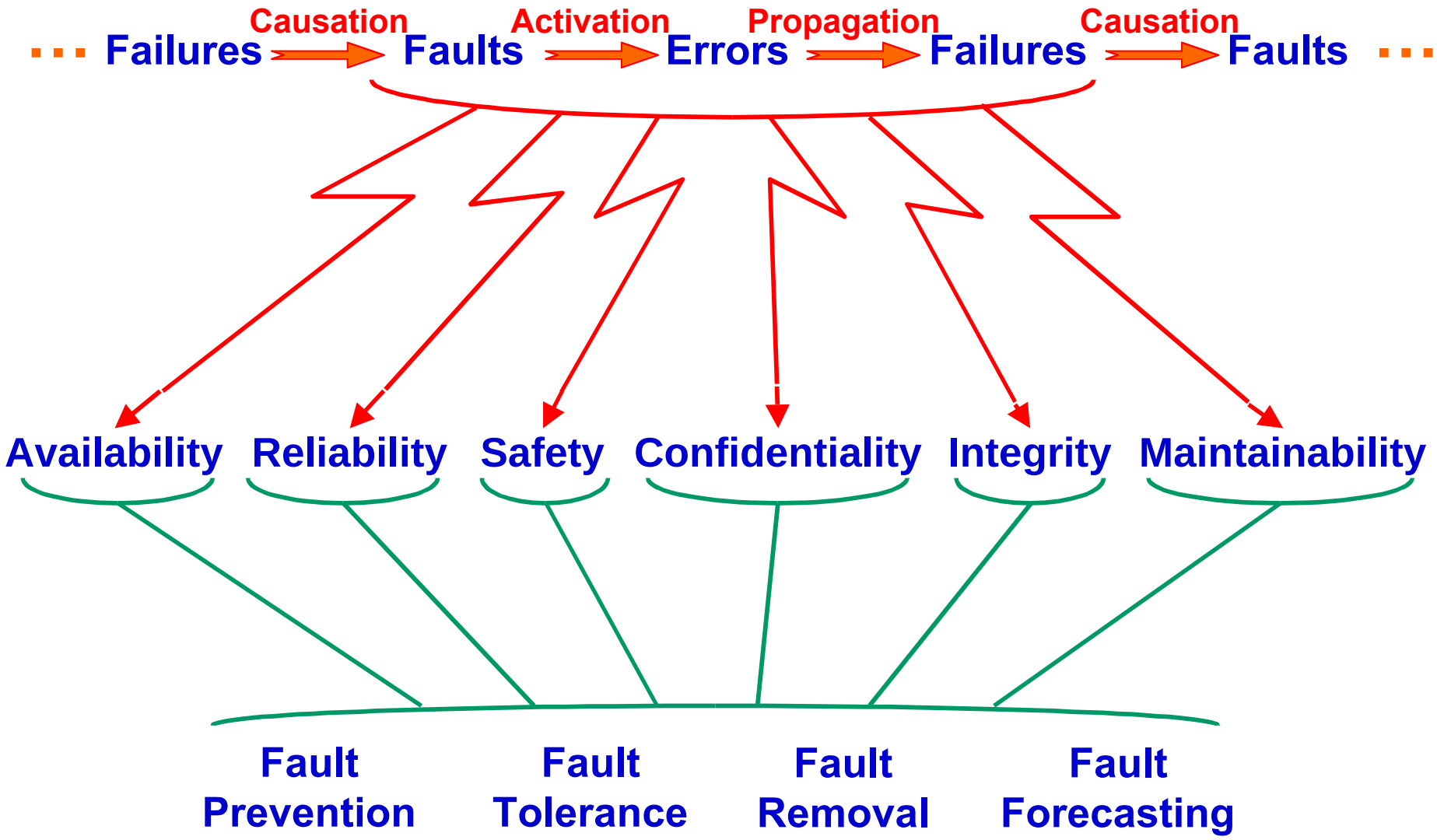
Dependability : ability to deliver service that can justifiably be trusted

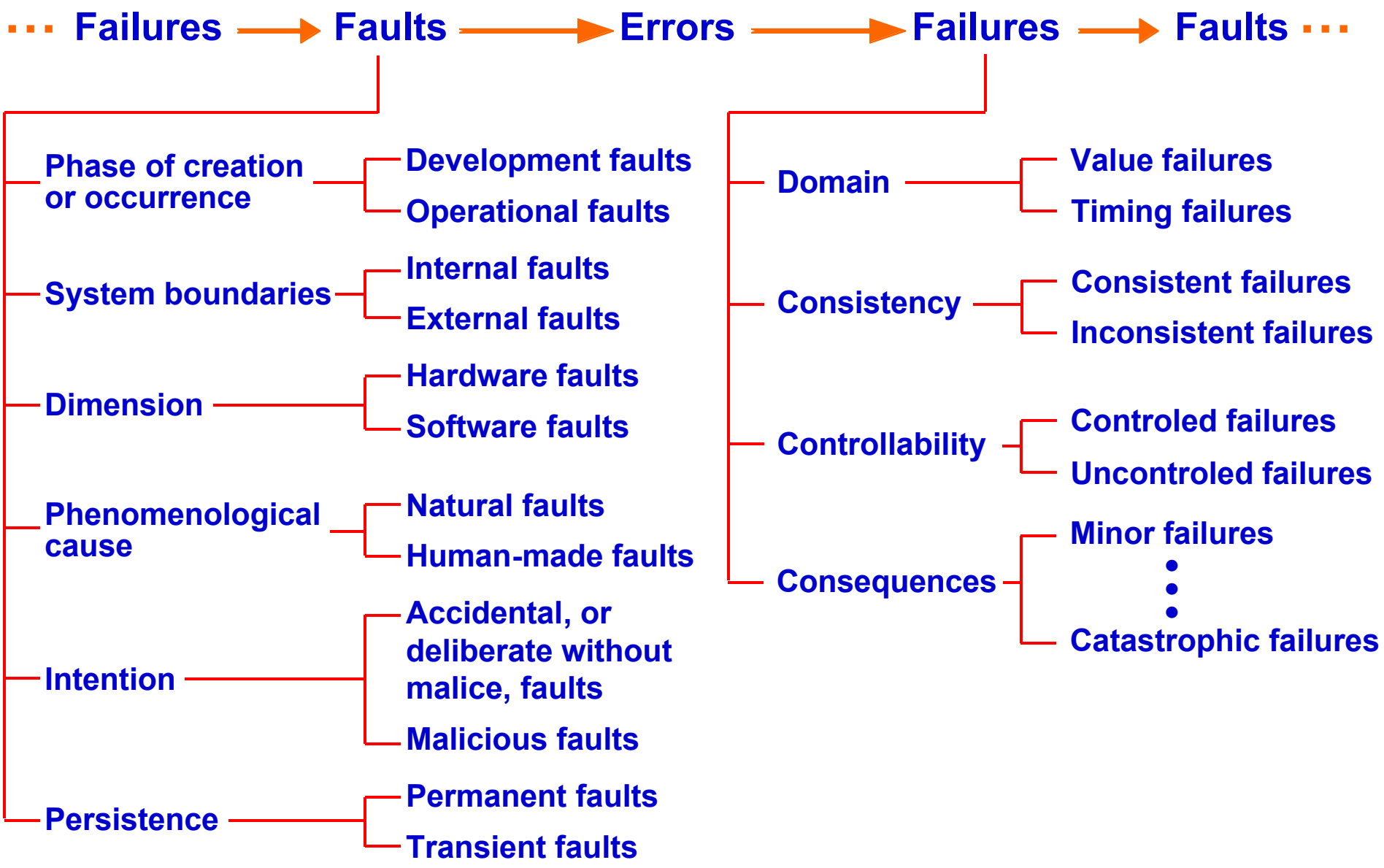
- Service delivered by a system: its behavior as it is perceived by its user(s)
- User: another system that interacts with the former
- Function of a system: what the system is intended to do
- (Functional) Specification: description of the system function
- Correct service: when the delivered service implements the system function
- System failure: event that occurs when the delivered service deviates from correct service, either because the system does not comply with the specification, or because the specification did not adequately describe its function
- Failure modes: the ways in which a system can fail, ranked according to failure severities

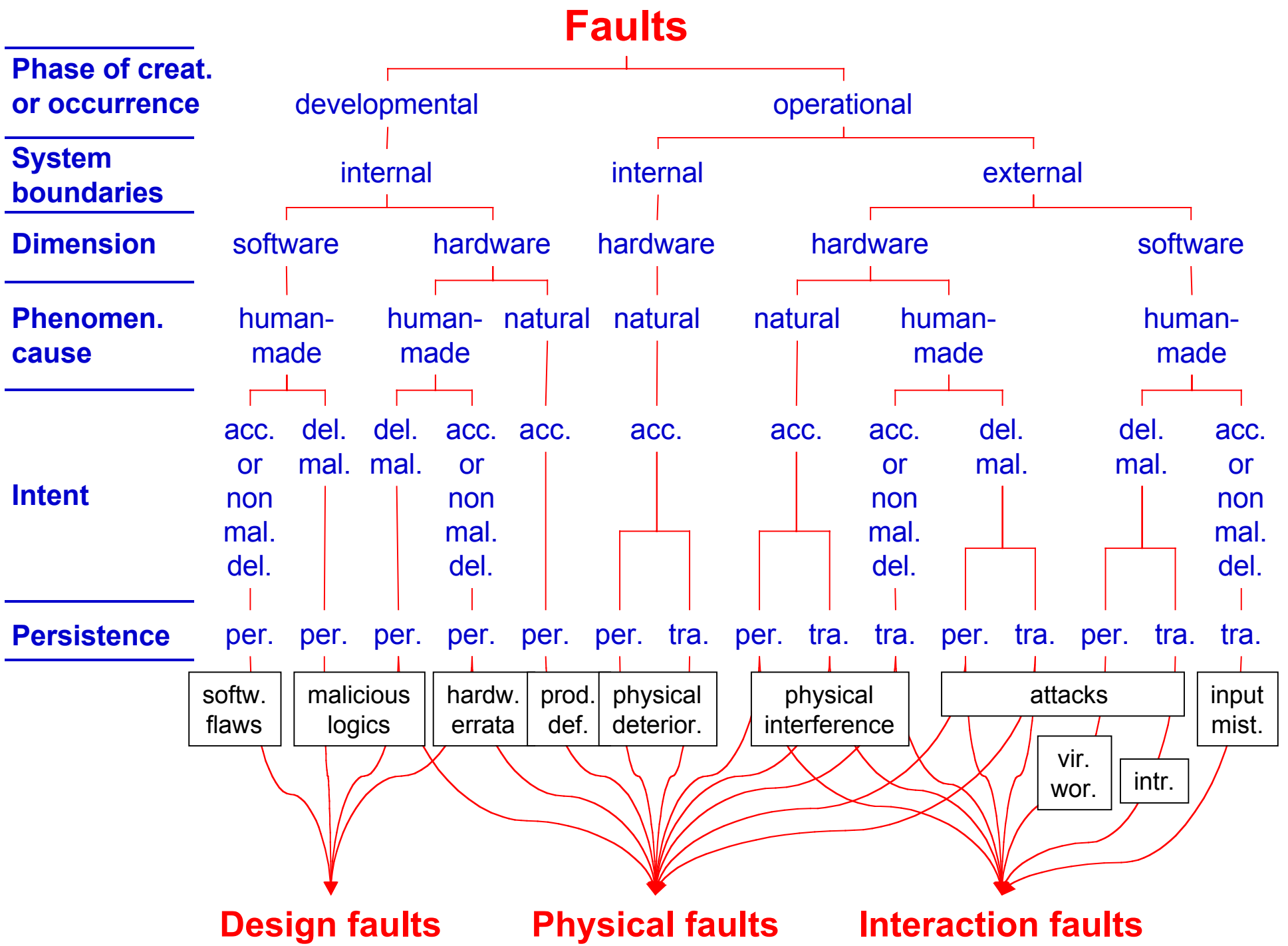
Dependability: ability to avoid failures that are more frequent or more severe than is acceptable to the user(s)

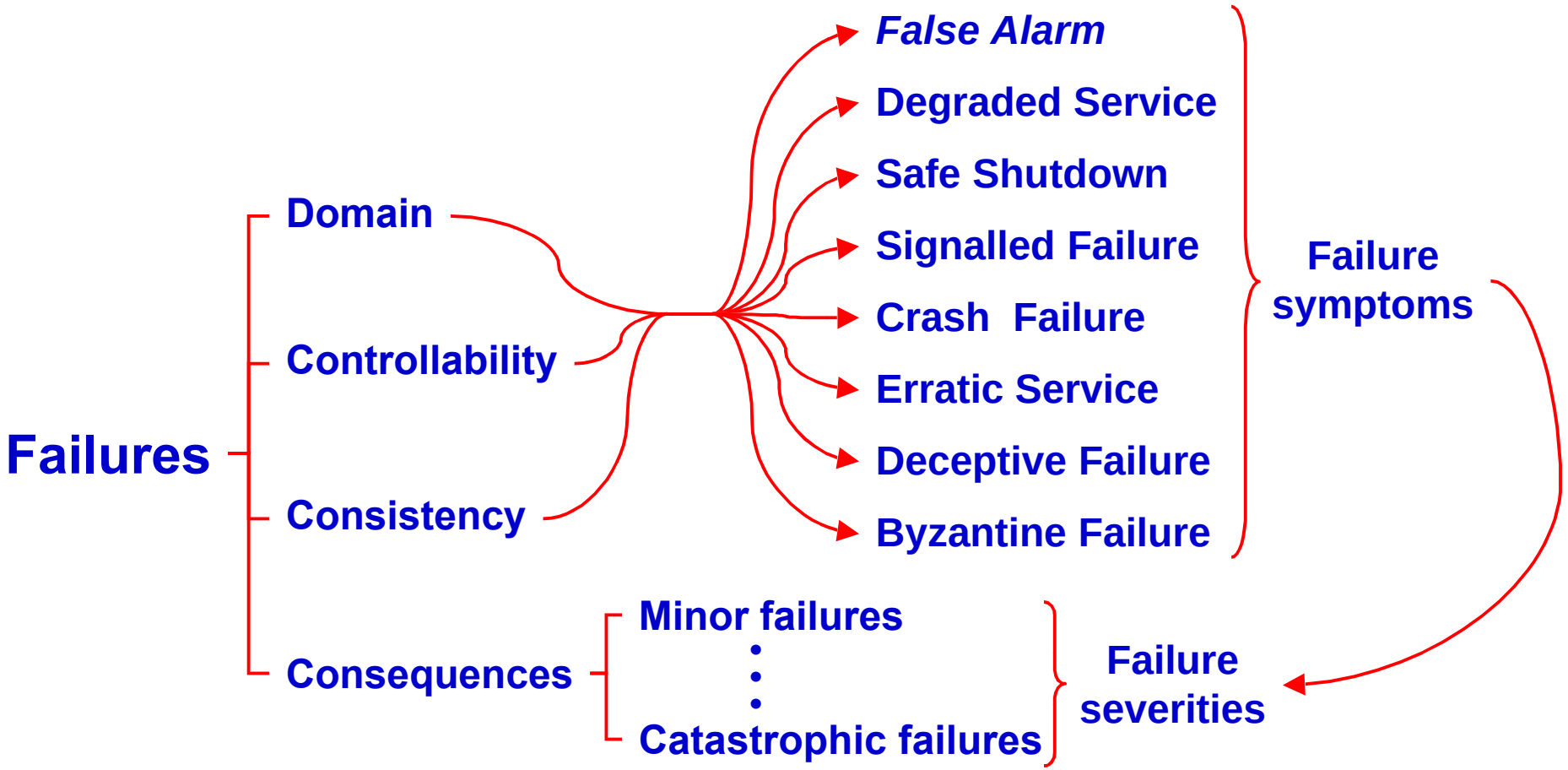
- When failures are more frequent or more severe than acceptable: meta-failure, i.e., a *dependability failure*

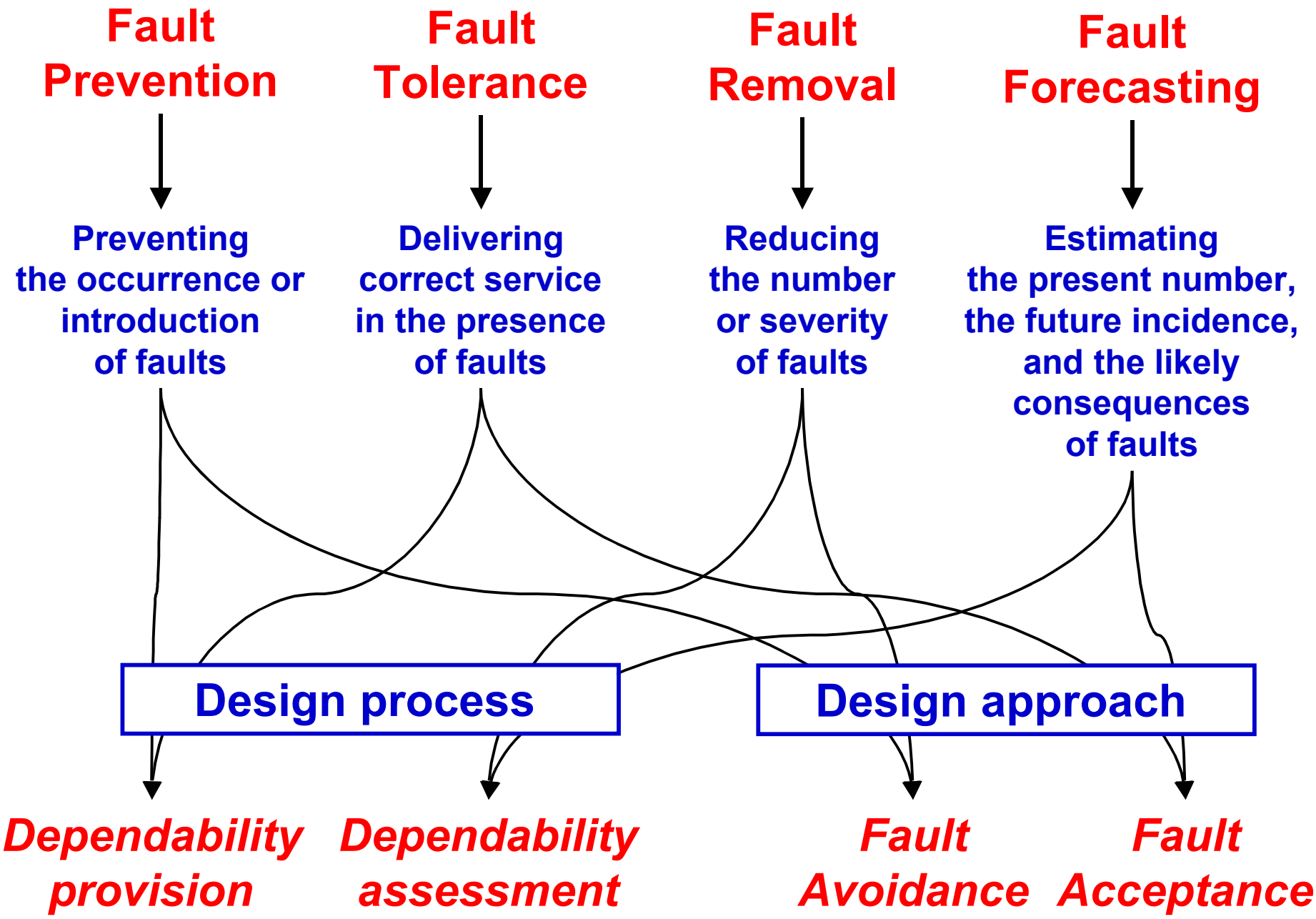

Dependability
Readiness for usage
Continuity of service
Absence of catastrophic consequences on the user(s) and the environment
Absence of unauthorized disclosure of information
Absence of improper system alterations
Ability to undergo repairs and evolutions
Availability
Reliability
Safety
Confidentiality
Integrity
Maintainability
Security
Absence of unauthorized access to, or handling of, system state

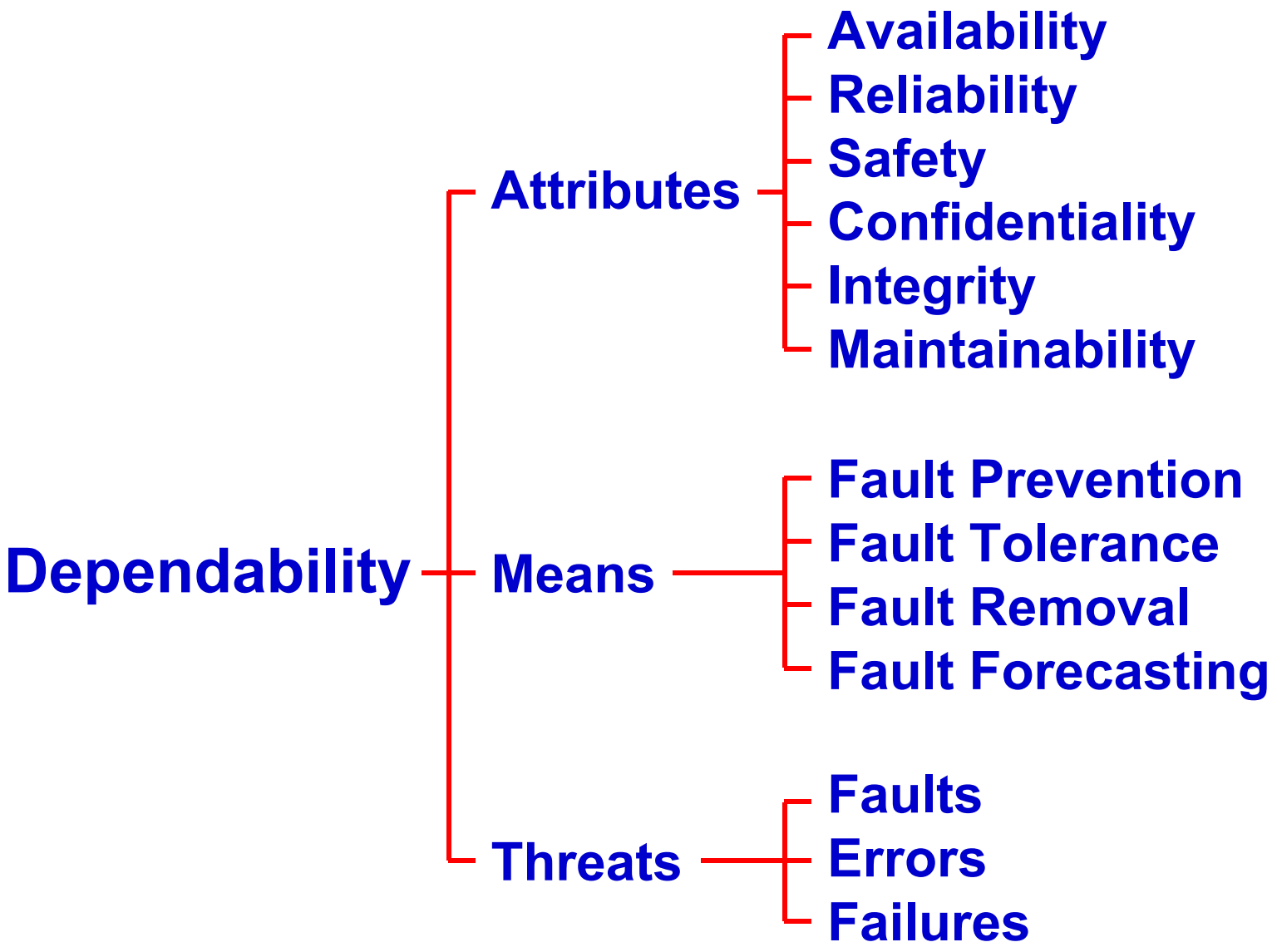

Causation
Activation
Propagation
Causation
Failures
Faults
Errors
Failures
Faults
Availability
Reliability
Safety
Confidentiality
Integrity
Maintainability
Fault Prevention
Fault Tolerance
Fault Removal
Fault Forecasting

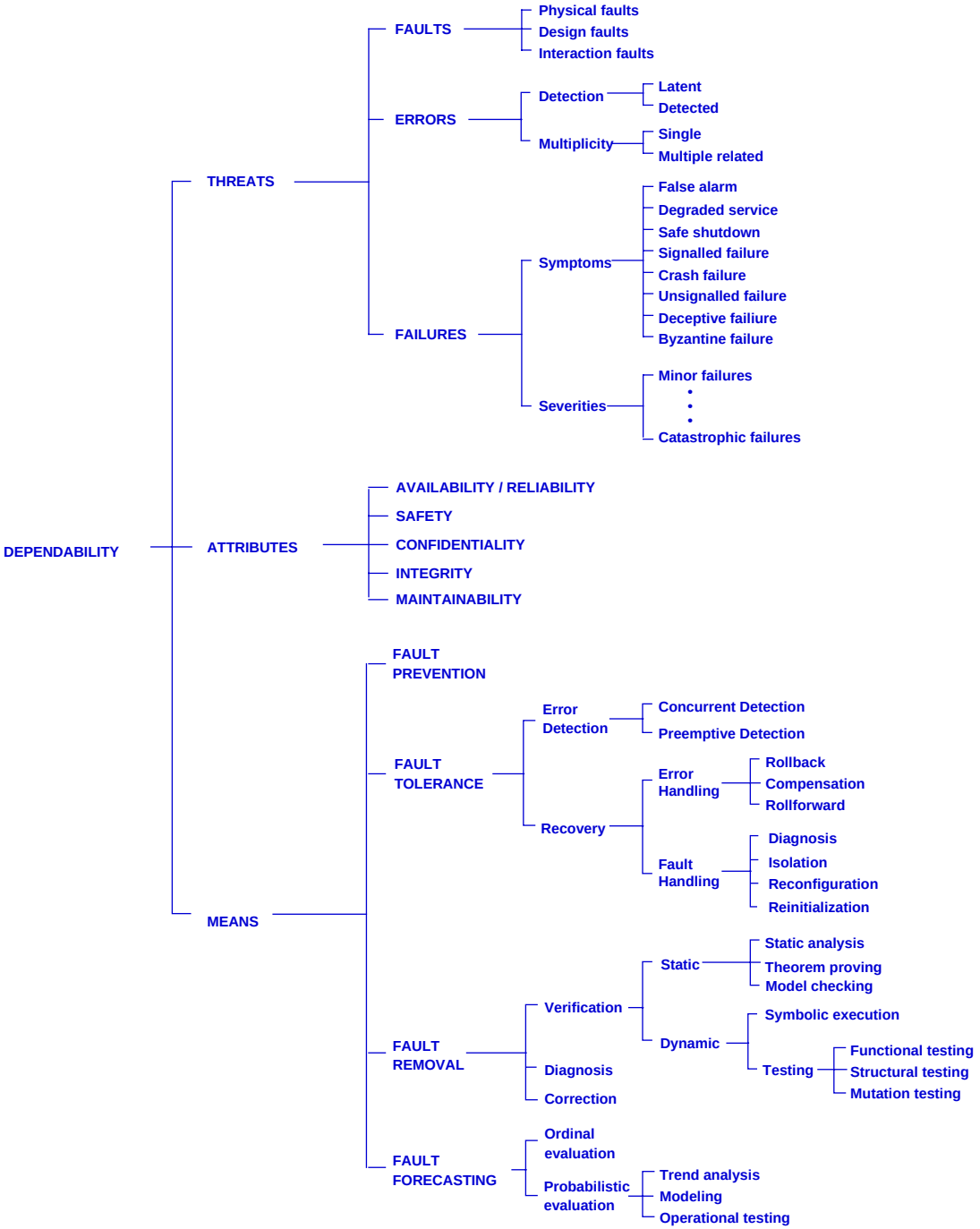

Failures
Faults
Errors
Failures
Faults
Phase of creation or occurrence
Development faults
Operational faults
System boundaries
Internal faults
External faults
Dimension
Hardware faults
Software faults
Phenomenological cause
Natural faults
Human-made faults
Intention
Accidental, or deliberate without malice, faults
Malicious faults
Persistence
Permanent faults
Transient faults
Domain
Value failures
Timing failures
Consistency
Consistent failures
Inconsistent failures
Controllability
Controled failures
Uncontroled failures
Consequences
Minor failures
Catastrophic failures


Faults
Phase of creat. or occurrence
System boundaries
Dimension
Phenomen. cause
Intent
Persistence
developmental
operational
internal
internal
external
software
hardware
hardware
hardware
software
human-made
human-made
natural
natural
natural
human-made
human-made
acc. or non mal. del.
del. mal.
del. mal.
acc. or non mal. del.
acc.
acc.
acc.
acc. or non mal. del.
del. mal.
del. mal.
acc. or non mal. del.
per.
per.
per.
per.
per.
per.
tra.
per.
tra.
tra.
per.
tra.
per.
tra.
tra.
softw. flaws
malicious logics
hardw. errata
prod. def.
physical deterior.
physical interference
attacks
vir. wor.
intr.
input mist.
Design faults
Physical faults
Interaction faults


Failures
Domain
Controllability
Consistency
Consequences
Minor failures
Catastrophic failures
False Alarm
Degraded Service
Safe Shutdown
Signalled Failure
Crash Failure
Erratic Service
Deceptive Failure
Byzantine Failure
Failure symptoms
Failure severities


Fault Prevention
Fault Tolerance
Fault Removal
Fault Forecasting
Preventing the occurrence or introduction of faults
Delivering correct service in the presence of faults
Reducing the number or severity of faults
Estimating the present number, the future incidence, and the likely consequences of faults
Design process
Design approach
Dependability provision
Dependability assessment
Fault Avoidance
Fault Acceptance


Dependability
Attributes
Availability
Reliability
Safety
Confidentiality
Integrity
Maintainability
Means
Fault Prevention
Fault Tolerance
Fault Removal
Fault Forecasting
Threats
Faults
Errors
Failures


DEPENDABILITY
THREATS
FAULTS
Physical faults
Design faults
Interaction faults
ERRORS
Detection
Latent
Detected
Multiplicity
Single
Multiple related
FAILURES
Symptoms
False alarm
Degraded service
Safe shutdown
Signalled failure
Crash failure
Unsignalled failure
Deceptive failiure
Byzantine failure
Severities
Minor failures
Catastrophic failures
ATTRIBUTES
AVAILABILITY / RELIABILITY
SAFETY
CONFIDENTIALITY
INTEGRITY
MAINTAINABILITY
MEANS
FAULT PREVENTION
FAULT TOLERANCE
Error Detection
Concurrent Detection
Preemptive Detection
Recovery
Error Handling
Rollback
Compensation
Rollforward
Fault Handling
Diagnosis
Isolation
Reconfiguration
Reinitialization
FAULT REMOVAL
Verification
Static
Static analysis
Theorem proving
Model checking
Dynamic
Symbolic execution
Testing
Functional testing
Structural testing
Mutation testing
Diagnosis
Correction
FAULT FORECASTING
Ordinal evaluation
Probabilistic evaluation
Trend analysis
Modeling
Operational testing

- **Dependability , survivability, trustworthiness: three names for an essential property**
- **All three concepts are essentially equivalent in their goals and address similar threats (trustworthiness omits the explicit listing of internal faults)**
- **Survivability was present in the late sixties in the military standards (*system capacity to resist hostile environments so that the system can fulfill its mission*)**
- **Threats are listed in the definitions of survivability and trustworthiness, while both definitions of dependability leave the choice open**