What is an Ontological Fault and why does it exist ?

Algirdas Avizienis
Distinguished Professor Emeritus, UCLA and
Rector Emeritus, Vytautas Magnus University, Lithuania

Research Report
IFIP WG 10.4 71st meeting, Queenstown, NZ
January 30, 2017

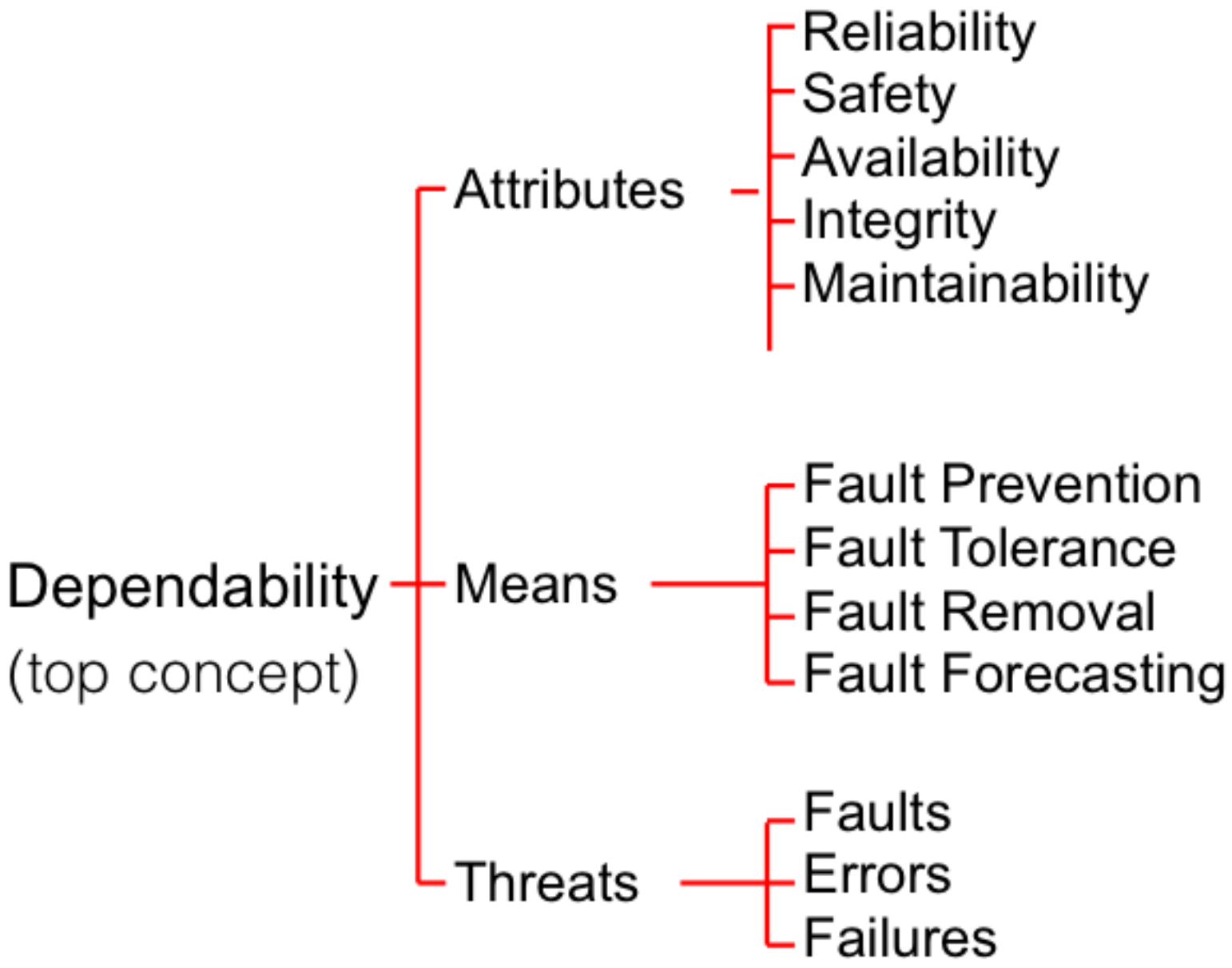
The Quantitative Definition of Dependability

The ***dependability*** (of a system)
is the ability to avoid service failures that are
(1) more frequent, and
(2) more severe
than is acceptable (to the user)

The Qualitative Definition of Dependability

The ***dependability*** (of a system)
is the ability deliver service
that can justifiably be trusted
(by the user)

The Dependability Taxonomy



A Crowded Field = A Real Mess

A ***dependable system*** delivers *expected service* (described by the *Attributes*) under *adverse circumstances* (described by the *Threats*) by using the *Means* to attain ***dependability.***

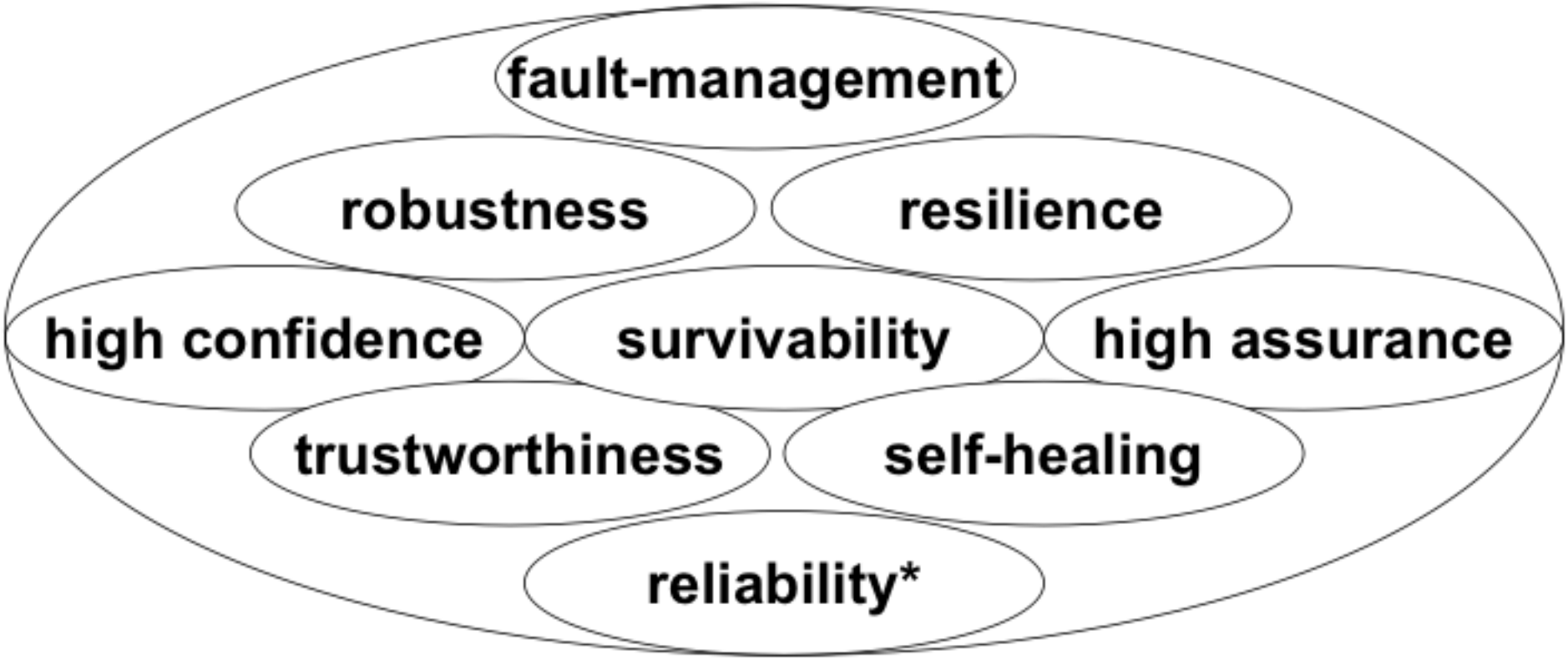
However, these systems are intended to do the same:
survivable, trustworthy, robust, high-confidence, reliable, high-assurance, self-healing, fault-managed, resilient

Are these ***top concepts*** equivalent or do they differ from dependability and/or among themselves ?

That is - ***how are they related ?*** We look for the answer by comparing their *taxonomies*.

Our Field's Objective: deliver expected service under adverse circumstances

Our Field's other Top Concepts:



****used as a top concept, not as an attribute of dependability***

Resilience as defined by J.-C. Laprie

in “From Dependability to Resilience”, Proc. DSN 2008, supplemental volume, Anchorage, AL, June 2008.

***Resilience* is the persistence of *dependability* when facing changes.”**

There are *3 dimensions of changes:*

1. their ***nature***: *functional, environmental, technological* (hardware and software)

2. their ***prospect:*** *foreseen* (new software versions), *foreseeable* (new hardware), *unforeseen* (new types of threats, new fault classes, etc.)

3. their ***timing***: *short term* (seconds to hours), *medium term* (hours to months, as in new versioning or reconfigurations), *long term* (months to years, as in merger of airline or banking information systems, or in military coalitions)

One More Threat: Ontological Fault

Each of these ***top concepts*** has appeared in the title of at least one international conference and in the titles and texts of numerous publications.

The absence of defined relationships between those top concepts is a major threat to the progress of our field - we call it an ***ontological fault.***

An ***ontology*** *is* a structured representation of the relationships between the concepts of a field. It may be seen as a taxonomy with more than one relationship, for example: inclusion plus causation.

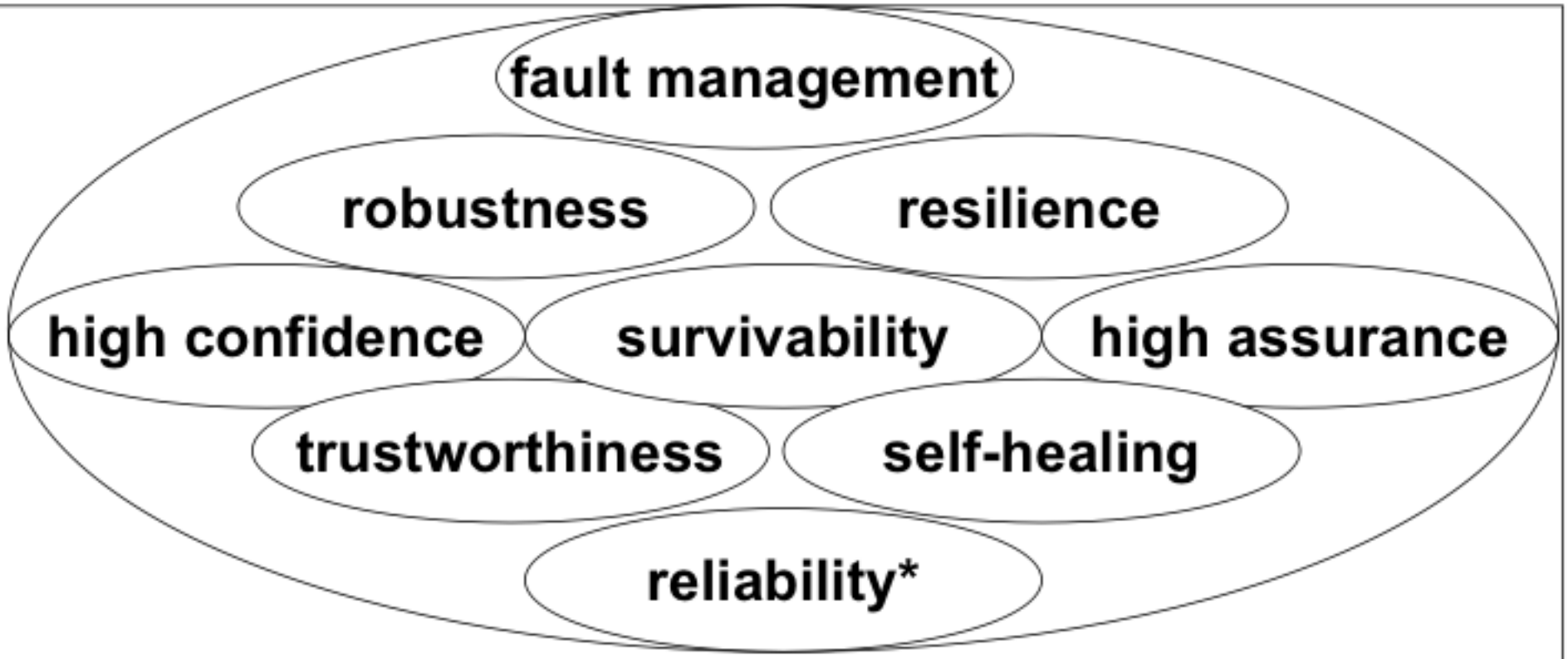
An ***ontological fault*** exists when the relationship of one top concept of a field to the others is not identified in a field that has two or more top concepts.

To search for taxonomy information about the *Top Concepts* shown below (and dependability) we have reviewed the

shown below (and dependability) we have reviewed the

ACM Computing Classification System, 2012 Revision

(abbreviated *ACM CCS* in the following slides)



***used as a top concept, not as an attribute of dependability**

ACM CCS: **(1)*General and reference***

(2) Cross-computing tools and techniques

(3) Reliability

Empirical studies

Measurement

Metrics

Evaluation

Experimentation

Estimation

Design

Performance

Validation

Verification

ACM CCS: **(1)*Hardware***

(2) Robustness

(3) Fault tolerance

(4) Error detection and error correction

Failure prediction

Failure recovery, maintenance and self-repair

Redundancy

Self-checking mechanisms

System-level fault tolerance

ACM CCS: **(1)** ***Hardware*** (continued)

(3) Hardware reliability

(4) Aging of circuits and systems

Circuit hardening

Transient errors and upsets

Early-life failures and infant mortality

Process, voltage and temperature variations

Signal integrity and noise analysis

(3) Safety critical systems

ACM CCS**: (1)*Computer systems organization***

(2) Dependable and fault-tolerant systems and networks

(3) Reliability

Availability

Maintainability and maintenance

Processors and memory architectures

Secondary storage organization

Redundancy

Fault-tolerant network topologies

ACM CCS:**(1)*Software and its engineering***

(2) Extra-functional properties

(3) Interoperability

Software performance

Software reliability

Software fault tolerance

(4) Checkpoint / restart

Software safety

Software usability

ACM CCS:**(1)** ***Networks***

(2) Network reliability

(3) Error detection and error correction

Conclusions about ACM CCS 2012:

1.The representation of our Field is very confused.

2.The concepts *Dependability, Resilience* are missing.

3.Only *Robustness and Reliability can be found of the ten *Top Concepts.***

4. Reliability* is not provided with any taxonomy

5. Robustness is a "catch-all" concept

One More Threat: Ontological Fault

Each of these ***top concepts*** has appeared in the title of at least one international conference and in the titles and texts of numerous

publications.

The absence of defined relationships between those top concepts is a major threat to the progress of our field - we call it an ***ontological fault.***

An ***ontology*** *is* a structured representation of the relationships between the concepts of a field. It may be seen as a taxonomy with more than one relationship, for example: inclusion plus causation.

An ***ontological fault*** exists when the relationship of one top concept of a field to the others is not identified in a field that has two or more top concepts.

Why ???

» To draw attention to a major problrm