A Visit to the Jungle of Terminology

Algirdas Avižienis
Vytautas Magnus University
Kaunas, Lithuania
avizienisa@gmail.com

***Abstract*—the goal of this short study is to compare nine widely used concepts: reliability, robustness, survivability, trustworthiness, high confidence, high assurance, fault management, self-healing, and resilience to the concept of dependability as it is presented with a taxonomy in the 2004 paper "Basic concepts and taxonomy of dependable and secure computing". The study also considers the representation of those concepts in the general taxonomy of computer science and engineering "ACM Computing Classification, 2012 Revision".**

I. Introduction: One Property with Ten Names

When a computing system, from a single microprocessor to a supercomputer or an entire network, is specified, designed, and built, it is required to deliver the expected services under certain adverse circumstances, usually called the *occurrence of faults*. From the time when the IEEE Computer Society Technical Committee on Fault-Tolerant Computing (1970) and the IFIP Working Group 10.4 "Reliable Computing and Fault Tolerance" (1980) were founded, their members were engaged in the development of a set of definitions and a taxonomy of dependable computing [1]. Later the concepts of secure computing were introduced, leading to the taxonomy presented in the comprehensive and widely cited paper [2].

The immediate problem that we faced in developing the taxonomy was that the widely used term *reliability* has two meanings, but only one can be used in building a taxonomy: (1) a general, broad concept of a desirable property, and (2) the precise mathematical concept of a probability $R(t)$ that service delivery is continuous from time $t = 0$ to time t. To solve this problem our choice was to select the term *dependability* for case (1), and to define *reliability* $R(t)$ as an attribute of *dependability* for case (2), as shown in Figure 1 that displays the first three levels of the taxonomy of *dependability* [2].

The concern with continuing to deliver expected service when faults occur exists in all fields of computer science and engineering, therefore at least eight other terms are also used to describe this system property. They are: *fault management, high assurance, high confidence, resilience, robustness, self-healing, survivability, trustworthiness*. In addition we have the two terms *dependability* and *reliability* discussed above. I will refer to these ten terms as Top-terms, abbreviated T-terms, because they would be the terms at the top level of their taxonomies, as *dependability* is in Figure 1. The current investigation is limited to *dependability*, excluding *security* (as it is defined in [2]) from consideration. Therefore *confidentiality* is not shown in Figure 1. The comparison of these T-terms with respect to *security* will be the next step of this investigation.

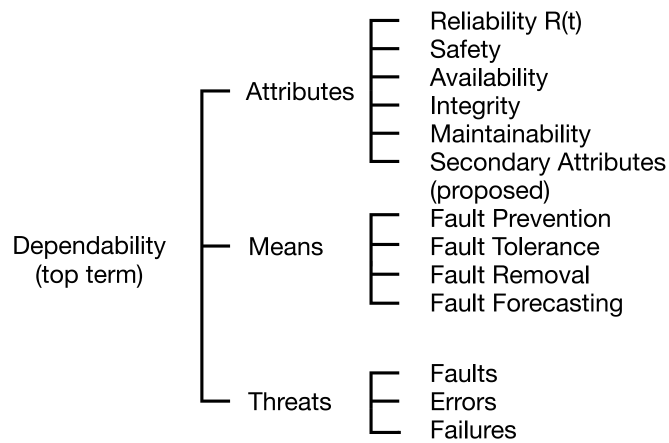

Fig. 1. The Dependability Taxonomy

II. A Comparison of Definitions

There exists a large number of published documents that use the ten T-terms being discussed here. In order to focus the study I use as sources the following documents: (1) the standards published by IEEE Standards Association; (2) publications by US Government agencies; and (3) the *"ACM Computing Classification System, 2012 Revision"* [3]. These documents were chosen because they have been created by major professional organizations or government agencies and contain stable consensus definitions. However, none of the references, except the ACM CCS, contains a taxonomy associated with the term that is being defined. The definitions I have selected are presented in Table 1.

There are two definitions of *dependability* and *reliability* each because the IEEE standard definitions in [4] differ from those in [2]. The T-term *resilience* is presented with three definitions because it is very widely used. In [2] it is identified as a synonym of fault tolerance, but later was defined as an extension of *dependability* by J.-C. Laprie [10]. He points out that the term was originally used in social psychology and materials science, and later elaborated in child psychology and psychiatry, in ecology, in organizational and business studies, and in industrial safety, the last presented as [12]. An extensive

TABLE I
THE DEFINITIONS OF TEN T-TERMS

T-term, [Source], Definition	Main Conference or Publication	Sponsor, Other Remarks
dependability [2]: (quantitative) the ability of a system to avoid service failures that are more frequent or more severe than is acceptable; (qualitative) the ability to deliver service that can justifiably be trusted	DSN 2016: the IEEE/IFIP International Conference on Dependable Systems and Networks	IEEE Computer Society TC on Dependable Computing and Fault Tolerance, and IFIP WG 10.4 on Dependability and Security
dependability [4]: (1) trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers; (2) availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance	IEEE Standard 24765-2010, "Systems and software engineering - Vocabulary"	(1) differs from [2] by using undefined term trustworthiness; (2) includes three attributes from [2] and maintenance support. Safety and integrity are not included.
reliability [2]: continuity of correct service: the probability $R(t)$ that correct service delivery is continuous from time $t = 0$ to time t	IEEE Transactions on Dependable and Secure Computing	$R(t)$ is an attribute of dependability in [2].
reliability [4]: (1) the ability of a system or component to perform its required functions under stated conditions for a specified period of time; (2) capability of the software product to maintain a specified level of performance when used under specified conditions	IEEE Standard 24765-2010, "Systems and software engineering - Vocabulary", IEEE Transactions on Reliability	(1) is a variation of $R(t)$, (2) refers to software "level of performance" that may be time-dependent. Term "reliability" is frequently used as a synonym for "dependability" in other publications.
robustness [4]: degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions	IEEE Standard 24765-2010, "Systems and software engineering - Vocabulary"	In [2] robustness is defined as a secondary attribute because it deals with external faults only.
survivability [4]: degree to which a product or system continues to fulfill its mission by providing essential services in a timely manner in spite of the presence of attacks	IEEE Standard 24765-2010, "Systems and software engineering - Vocabulary"	Originally a US military standard, later developed by SEI at CMU in the context of survivable networks. The term attacks implies security as the primary concern.
trustworthiness [5]: trustworthy systems are reliable, usable, interoperable and secure.	*Trust in Cyberspace*, F. Schneider, ed., National Academy Press, 1999	Based on NRC study, the term is security-oriented. Includes usability and interoperability as explicit attributes. Favored by NIST.
high confidence [6]: this term encompasses the behavior of hardware, software, and systems (devices) regardless of size or complexity, plus all interconnections; high-confidence systems are robust (manage failures) and can justifiably be trusted, especially when used in life-, safety-, security, and mission-critical situations	High Confidence Software and Systems Conference HCSS 2016 (www.cps-vo.org/node/25173/)	Favored by US multiagency NITRD (Networking and Information Technology R&D) program. HCSS is organized by Cyber-Physical Systems - Virtual Organization (CPS-VO).
high assurance [7]: high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties	HASE 2016: 17th IEEE International Symposium on High Assurance Systems Engineering conference	Term favored by DARPA and other US military R&D programs.
fault management [8]: the engineering discipline that encompasses practices that enables operational system to contain, prevent, detect, isolate, diagnose, respond to, and recover from conditions that may interfere with nominal mission operations	"Fault Management Handbook", NASA-HDBK-1002, April 2012, www.nasa.gov	Term developed and favored by NASA.
self-healing [9]: self-healing can be defined as the property that enables a system to perceive that it is not operating correctly and, without (or with) human intervention, make the necessary adjustments to restore itself to normalcy	DASC 2016 : Dependable Autonomic and Secure Computing	In [2] self-healing is identified as a synonym of fault tolerance. The term originated in communications research in the 80s, later was reintroduced by IBM as part of the Autonomic Computing initiative.
resilience [10]: the persistence of dependability when facing changes	European Network of Excellence ReSIST: Resilience for Survivability in IST, www.resist-noe.org	The changes are classified in three dimensions: their nature, prospect, and timing. The term *resilience* was identified as a synonym of fault tolerance in [2].
resilience [11]: resilience is understood as the ability of a system to anticipate, withstand, recover, and evolve from cyber attacks and failures	International Symposium on Resilient Cyber Systems, Resilience Week 2017	Organizers: IEEE Industrial Electronics Society and Idaho National Laboratory
resilience [12]: the capability - how well can a system handle disruptions and variations that fall outside of the base mechanisms/model for being adaptive as defined in that system	"Resilience Engineering", E. Hollnagel, D.D. Woods, and N. Leveson, editors, Ashgate Publishing, Ltd., 2012.	Concerns industrial safety and organizational resilience. "Adaptive" corresponds to "dependable" in [10].

use of *resilience* in several contexts is found in the annual *"Resilience Week"* conference [11].

The common goal of all ten system properties (T-terms) of Table 1 is to avoid service failures when affected by threats and to recover rapidly if a service failure occurs. The question I address here is: do the other nine T-terms differ from *dependability*? The conclusive answer would be obtained by comparing their taxonomies to that of *dependability*. If the attributes, means, and threats (AMTs) are the same the answer is *NO*, otherwise it is *YES*: there are different AMTs, or some AMTs are missing, or both. However, since I was not able to find taxonomies of the other T-terms, the answer must be found by comparing the definitions of Table 1.

The comparison of the nine definitions to *dependability* is difficult because they are presented exactly as they were in the referenced documents and are very diverse in their styles and lengths. While every definition states the goal, the number of attributes, means, and threats (AMTs) stated in a definition differs greatly - from several to none at all. Of course, the absence of an AMT in the definition may mean that it is considered to be of *"secondary"* significance.

The comparison of the AMTs in each definition to the AMTs of the taxonomy of Figure 1 shows that only the attributes *usable* and *interoperable* in *trustworthiness*[5] do not explicitly appear in the taxonomy of [2]. Implicitly there they are *secondary attributes*. All other AMTs are contained in the taxonomy of [2], therefore I hypothesize that the taxonomy of *dependability* would include the taxonomies of the other nine T-terms.

It was stated in the Introduction that the study of the T-term *security* in [2] was deferred for the next stage of this investigation. It is noted that *security* appears in the definitions: *trustworthiness* [5], *high confidence* [6], and *high assurance* [7], while the threat *"attacks"* is found in *survivability* [4] and *resilience* [11].

III. Search for T-term taxonomies in the ACM CCS

Since the search for authoritative taxonomies of the T-terms of Table 1 has not yielded any results, the remaining possibility is to search for those taxonomies that may exist as parts of the *"ACM Computing Classification System, 2012 Revision"* (abbreviated *ACM CCS*) which is a general taxonomy for all of computer science and engineering [3].

The (1) ACM CCS is a six-level taxonomy. The (1) in front indicates that *"ACM CCS"* is the first-level (top) term.The second level consists of 14 terms that cover the entire field. Those terms are distinguished by bold letters, such as: (2) **General and reference**, (2) **Hardware**, etc. Terms from the other levels also are marked with their level. Terms that are T-terms from Table 1 are distinguished by italic letters: (4) *Reliability*, (3) *Robustness*, (3) *Dependable*. Their segments from (1) *ACM CCS* are shown in Figures 2, 3, and 4.

The main conclusion about the content of the ACM CCS taxonomy is that the domain of the T-term *dependability* [2] is very poorly represented and is useless for our study. The worst shortcoming is the failure to distinguish between the term

(2) **General and reference**
- (3) Cross-computing tools and techniques
  - (4) *Reliability*
    - Empirical studies
    - Measurement
    - Metrics
    - Evaluation
    - Experimentation
    - Estimation
    - Design
    - Performance
    - Validation
    - Verification

Fig. 2. "Reliability" in ACM CCS

(2) **Computer systems organization**
- (3) *Dependable* and fault-tolerant systems and networks
  - (4) Reliability
    - Availability
    - Maintainability and maintenance
    - Secondary storage organization
    - Redundancy
    - Fault-tolerant network topologies

Fig. 3. "Dependable" in ACM CCS

(2) **Hardware**
- (3) *Robustness*
  - (4) Fault tolerance
    - (5) Error detection and error correction
      - Failure prediction
      - Failure recovery, maintenance and self-repair
      - Redundancy
      - Self-checking mechanisms
      - System-level fault tolerance
  - (4) Design for manufacturability
    - (5) Process variations
      - Yield and cost modeling
      - Yield and cost optimization
  - (4) Hardware reliability
    - (5) Aging of circuits and systems
      - Circuit hardening
      - Early-life failures and infant mortality
      - Process, voltage and temperature variations
      - Signal integrity and noise analysis
      - Transient errors and upsets
  - (4) Safety critical systems

Fig. 4. "Robustness" in ACM CCS

"reliability" treated as a general concept, and the attribute $R(t)$ that is a probabilistic measure of the continuity of expected service delivery (see Figure 1). The problem can be resolved by substituting the T-term (4) *Dependability* for (4) *Reliability* in the (2) **General and reference** domain (Figure 2) and elsewhere where "reliability" is intended to be the general concept. That was the solution adopted in [2]. It is unclear why this solution was not accepted by authors of the *ACM CCS* revision of 2012, since [2] was published in 2004 and had been very widely used and cited by 2012.

The T-term *dependability* does not appear in the ACM CCS. It is represented by its adjective form in (3) *Dependable* and fault-tolerant systems and networks at level (3) of (2) **Computer systems organization** (Figure 3). The level (4) terms (4)Reliability, (4)Availability, and (4)Maintainability and maintenance, correspond to three attributes of Figure 1, but the other four terms at the level (4) seem to be rather arbitrarily chosen. They are: (4)Processors and memory architectures, (4)Secondary storage organization, (4)Redundancy, and (4)Fault-tolerant network topologies.

The only other T-term that appears in the ACM CCS is (3) *Robustness* at level (3) of (2) **Hardware** (Figure 4). It has four level (4) terms: (4) Fault tolerance, (4)Design for manufacturability, (4) Hardware reliability, (4) Safety critical systems. The term (4) Fault tolerance has three level (5) terms that definitely involve software and do not belong here, for example: (5) Failure recovery, (5) Maintenance and self-repair, and (5) System-level fault tolerance.

Another aspect of fault tolerance: (5) Software fault tolerance appears at level (5) of (2) **Software and its engineering**. "Fault tolerance" is included under three top terms and lacks the cohesiveness of its treatment as a means of dependability in [2]. Finally, the seven widely used T-terms *survivability, resilience, trustworthiness, fault management, high confidence, self-healing*, and *high assurance* do not appear at all in the ACM CCS. The choice of the T-term (3) *Robustness* instead of another one from those seems arbitrary.

IV. In Conclusion: What Did I Find?

The goal of this study was to determine the relationships of nine widely used concepts: *reliability, robustness, survivability, trustworthiness, high confidence, high assurance, fault management, self-healing*, and *resilience* (called "T-terms" in this paper) with the concept of *dependability* as it was presented in [2]. The concept of *security* from [2] was not included in the present study in order to limit its extent.

The method used was to find authoritative definitions of those nine concepts and to determine if the definitions contained terms that were not included in the taxonomy of *dependability* presented in [2]. Finding complete taxonomies to compare would lead to more conclusive results, but I did not succeed in my search.

The principal result of the study is that I did not discover threats, means, and attributes that were not included in the taxonomy of [2], with only one exception: *trustworthiness* [5] requires the attributes *usability* and *interoperability* that are not included among the attributes of *dependability* in [2].

Given this result I propose the hypothesis that the taxonomies of the nine T-terms would be subsets of the *dependability* [2] taxonomy in [2], with the exception for *trustworthiness* [5]. To avoid such exceptions I recommend that the taxonomy of [2] should be augmented by adding secondary attributes *usability* and *interoperability* as well as other secondary attributes of *dependability*.

A second result was the observation that the ACM CCS taxonomy fails to include seven T-terms. *ACM CCS* sections for (4) *Reliability*, (3) *Robustness* and (3) *dependable and fault-tolerant systems and networks* are shown in Figures 2, 3, and 4. Regrettably, many entries seem to be rather arbitrarily chosen and do not reflect the orderly approach of the taxonomy in [2]. It is my intent to send these observations to the editor of the *ACM CCS* and suggest some improvements.

V. Acknowledgments

I thank my colleagues in IFIP WG 10.4 for many pleasant and productive discussions of the terminology jungle and the ways out of it. In advance I thank all colleagues who will send their suggestions how this study can be improved. Please send more comprehensive (but authoritative) definitions, and point out taxonomies that I have not been able to find. Many thanks to Rimas Avižienis for his help in putting this paper into a reasonably legible and comprehensible form.

VI. References

[1] Laprie, J.C., Costes, A., "Dependability: a unifying concept for reliable computing", Proceedings FTCS-12, Santa Monica, CA, June 1982, pp. 18-21

[2] Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C., "Basic concepts and taxonomy of dependable and secure computing", IEEE Trans. On Dependable and Secure Computing, vol.1, no.1, 2004, pp. 11-33

[3] "ACM Computing Classification, 2012 Revision", www.acm.org/ccs

[4] IEEE standard 24765-2010,"Systems and software engineering - Vocabulary", December 2010, www.computer.org/sevocab

[5] "Trustworthy Information Systems", NIST Information Technology Laboratory, January 2011, www.nist.gov/itl

[6] "High-Confidence Medical Devices", NITRD Research and Development Needs Report, February 2009, www.nitrd.gov

[7] Richards, R., "High Assurance Cyber Military Systems (HACMS)", DARPA Program Information, Dec. 2016, www.darpa.gov

[8] "Fault Management Handbook", NASA-HDBK-1002, April 2012, www.nasa.gov

[9] Ghosh, D. et al., "Self-healing systems - survey and synthesis", www.sciencedirect.com, August 2006

[10] Laprie, J.-C., "From dependability to resilience", Proceedings of DSN 2008, supplemental volume, Anchorage, AL, June 2008.

[11] "Resilience Week 2017", www.resilienceweek.com

[12] "Chapter 2: Essential Characteristics of Resilience" by David D. Woods in *"Resilience Engineering"*, E. Hollnagel, D.D. Woods, and N. Leveson, editors, Ashgate Publishing, Ltd., 2012, p.28.