

Glossary of terms used in Software Testing

Version 1.0 (dd. December, 8th 2004)

**Produced by the ‘Glossary Working Party’
International Software Testing Qualification Board**

Editor : Erik van Veenendaal

Contributors : Sigrid Eldh, Isabel Evans, Dorothy Graham, Julian Harty,
David Hayman, Juha Itkonen Vipul Kocher, Fernando Lamas de
Oliveira, Tilo Linz, Peter Morgan, Thomas Müller, Avi Ofer,
Dale Perry, Horst Pohlmann, Meile Posthuma, Erkki Pöyhönen
Maaret Pyhäjärvi, Andy Redwood, Stuart Reid, Hans Schaefer,
Jurriën Seubers, Dave Sherrat, Mike Smith, Andreas Spillner,
Richard Taylor, Geoff Thompson, Matti Vuori, Stephanie
Ulrich, Pete Williams

Copyright Notice

This document may be copied in its entirety, or extracts made, if the source is acknowledged.

Table of Content

Foreword.....	3
1. Introduction.....	3
2. Scope	3
3. Arrangement	3
4. Normative references	4
5. Definitions	4
A.....	4
B.....	5
C.....	7
D.....	10
E.....	12
F.....	13
G.....	15
H.....	15
I.....	15
K.....	17
L.....	17
M.....	17
N.....	19
O.....	19
P.....	19
Q.....	21
R.....	21
S.....	23
T.....	26
U.....	30
V.....	30
W	31
Annex A (Informative).....	32
Annex B (Method of commenting on this glossary)	33

Foreword

In compiling this glossary the working party has sought the views and comments of as broad a spectrum of opinion as possible in industry, commerce and government bodies and organizations, with the aim of producing an international testing standard which would gain acceptance in as wide a field as possible. Total agreement will rarely, if ever, be achieved in compiling a document of this nature. Contributions to this glossary have been received from the testing communities in Australia, Belgium, Finland, Germany, India, Israel, The Netherlands, Norway, Portugal, Sweden, United Kingdom, and USA.

Many (software) testers have used BS 7925-1 since its original publication in 1998. It has served also as a major reference for the Information Systems Examination Board (ISEB) qualifications at both Foundation and Practitioner level. The standard was initially developed with a bias towards component testing, but, since its publication, many comments and proposals for new definitions have been submitted to both improve and expand the standard to cover a wider range of software testing. In this new version of the testing glossary many of these suggested updates have been incorporated. It will be used as a reference document for the International Software Testing Qualification Board (ISTQB) software testing qualification scheme.

1. Introduction

Much time and effort is wasted both within and between industry, commerce, government and professional and academic institutions when ambiguities arise as a result of the inability to differentiate adequately between such terms as ‘statement coverage’ and ‘decision coverage’; ‘test suite’, ‘test specification’ and ‘test plan’ and similar terms which form an interface between various sectors of society. Moreover, the professional or technical use of these terms is often at variance with different meanings attributed to them.

2. Scope

This document presents concepts, terms and definitions designed to aid communication in (software) testing and related disciplines.

3. Arrangement

The glossary has been arranged in a single section of definitions ordered alphabetically. Some terms are preferred to other synonymous ones, in which case, the definition of the preferred term appears, with the synonymous ones referring to that. For example *structural testing* refers to *white box testing*. For synonyms, the “See” indicator is used

“See also” cross-references are also used. They assist the user to quickly navigate to the right index term. “See also” cross-references are constructed for relationships such as broader term to a narrower term, and overlapping meaning between two terms.

4. Normative references

At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based upon this Standard are encouraged to investigate the possibility of applying the most recent edition of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

- BS 7925-2:1998. Software Component Testing.
- DO-178B:1992. Software Considerations in Airborne Systems and Equipment Certification, Requirements and Technical Concepts for Aviation (RTCA SC167).
- IEEE 610.12:1990. Standard Glossary of Software Engineering Terminology.
- IEEE 829:1998. Standard for Software Test Documentation.
- IEEE 1008:1993. Standard for Software Unit Testing.
- IEEE 1012:1986. Standard for Verification and Validation Plans
- IEEE 1028:1997. Standard for Software Reviews and Audits.
- IEEE 1044:1993. Standard Classification for Software Anomalies.
- IEEE 1219:1998. Software Maintenance.
- ISO/IEC 2382-1:1993. Data processing - Vocabulary - Part 1: Fundamental terms.
- ISO 9000:2000. Quality Management Systems – Fundamentals and Vocabulary.
- ISO/IEC 9126-1:2001. Software Engineering – Software Product Quality – Part 1: Quality characteristics and sub-characteristics.
- ISO/IEC 12207:1995. Information Technology – Software Life Cycle Processes.
- ISO/IEC 14598-1:1996. Information Technology – Software Product Evaluation - Part 1: General Overview

5. Definitions

A

abstract test case: See high level test case.

acceptance: See acceptance testing.

acceptance criteria: The exit criteria that a component or system must satisfy in order to be accepted by a user, customer, or other authorized entity. [IEEE 610]

acceptance testing: Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system. [After IEEE 610]

accessibility testing: Testing to determine the ease by which users with disabilities can use a component or system. [Gerrard]

accuracy: The capability of the software product to provide the right or agreed results or effects with the needed degree of precision. [ISO 9126] See also functionality testing.

actual outcome: See actual result.

actual result: The behavior produced/observed when a component or system is tested.

ad hoc review: See informal review.

ad hoc testing: Testing carried out informally; no formal test preparation takes place, no recognized test design technique is used, there are no expectations for results and randomness guides the test execution activity.

adaptability: The capability of the software product to be adapted for different specified environments without applying actions or means other than those provided for this purpose for the software considered. [ISO 9126] See also portability testing.

agile testing: Testing practice for a project using agile methodologies, such as extreme programming (XP), treating development as the customer of testing and emphasizing the test-first design paradigm.

algorithm test [TMap]: See branch testing.

alpha testing: Simulated or actual operational testing by potential users/customers or an independent test team at the developers' site, but outside the development organization. Alpha testing is often employed as a form of internal acceptance testing.

analyzability: The capability of the software product to be diagnosed for deficiencies or causes of failures in the software, or for the parts to be modified to be identified. [ISO 9126] See also maintainability testing.

analyzer: See static analyzer.

anomaly: Any condition that deviates from expectation based on requirements specifications, design documents, user documents, standards, etc. or from someone's perception or experience. Anomalies may be found during, but not limited to, reviewing, testing, analysis, compilation, or use of software products or applicable documentation. [IEEE 1044] See also defect, deviation, error, fault, failure, incident, problem.

arc testing: See branch testing.

attractiveness: The capability of the software product to be attractive to the user. [ISO 9126] See also usability testing.

audit: An independent evaluation of software products or processes to ascertain compliance to standards, guidelines, specifications, and/or procedures based on objective criteria, including documents that specify:

- (1) the form or content of the products to be produced
- (2) the process by which the products shall be produced
- (3) how compliance to standards or guidelines shall be measured. [IEEE 1028]

audit trail: A path by which the original input to a process (e.g. data) can be traced back through the process, taking the process output as a starting point. This facilitates defect analysis and allows a process audit to be carried out. [After TMap]

automated testware: Testware used in automated testing, such as tool scripts.

availability: The degree to which a component or system is operational and accessible when required for use. Often expressed as a percentage. [IEEE 610]

B

back-to-back testing: Testing in which two or more variants of a component or system are executed with the same inputs, the outputs compared, and analyzed in cases of discrepancies. [IEEE 610]

baseline: A specification or software product that has been formally reviewed or agreed upon, that thereafter serves as the basis for further development, and that can be changed only through a formal change control process. [After IEEE 610]

basic block: A sequence of one or more consecutive executable statements containing no branches.

basis test set: A set of test cases derived from the internal structure or specification to ensure that 100% of a specified coverage criterion is achieved.

bebugging: See error seeding. [Abbott]

behavior: The response of a component or system to a set of input values and preconditions.

benchmark test: (1) A standard against which measurements or comparisons can be made.
(2) A test that is be used to compare components or systems to each other or to a standard as in (1). [After IEEE 610]

bespoke software: Software developed specifically for a set of users or customers. The opposite is off-the-shelf software.

best practice: A superior method or innovative practice that contributes to the improved performance of an organization under given context, usually recognized as ‘best’ by other peer organizations.

beta testing: Operational testing by potential and/or existing users/customers at an external site not otherwise involved with the developers, to determine whether or not a component or system satisfies the user/customer needs and fits within the business processes. Beta testing is often employed as a form of external acceptance testing in order to acquire feedback from the market.

big-bang testing: A type of integration testing in which software elements, hardware elements, or both are combined all at once into a component or an overall system, rather than in stages. [After IEEE 610] See also integration testing.

black box technique: See black box test design technique.

black box testing: Testing, either functional or non-functional, without reference to the internal structure of the component or system.

black box test design techniques: Documented procedure to derive and select test cases based on an analysis of the specification, either functional or non-functional, of a component or system without reference to its internal structure.

blocked test case: A test case that cannot be executed because the preconditions for its execution are not fulfilled.

bottom-up testing: An incremental approach to integration testing where the lowest level components are tested first, and then used to facilitate the testing of higher level components. This process is repeated until the component at the top of the hierarchy is tested. See also integration testing.

boundary value: An input value or output value which is on the edge of an equivalence partition or at the smallest incremental distance on either side of an edge, for example the minimum or maximum value of a range.

boundary value analysis: A black box test design technique in which test cases are designed based on boundary values.

boundary value coverage: The percentage of boundary values that have been exercised by a test suite.

boundary value testing: See boundary value analysis.

branch: A basic block that can be selected for execution based on a program construct in which one of two or more alternative program paths are available, e.g. case, jump, go to, if-then-else.

branch condition: See condition.

branch condition combination coverage: See multiple condition coverage.

branch condition combination testing: See multiple condition testing.

branch condition coverage: See condition coverage.

branch coverage: The percentage of branches that have been exercised by a test suite. 100% branch coverage implies both 100% decision coverage and 100% statement coverage.

branch testing: A white box test design technique in which test cases are designed to execute branches.

bug: See defect.

business process-based testing: An approach to testing in which test cases are designed based on descriptions and/or knowledge of business processes.

C

Capability Maturity Model (CMM): A five level staged framework that describes the key elements of an effective software process. The Capability Maturity Model covers practices for planning, engineering and managing software development and maintenance. [CMM]

Capability Maturity Model Integration (CMMI): A framework that describes the key elements of an effective product development and maintenance process. The Capability Maturity Model Integration covers practices for planning, engineering and managing product development and maintenance. CMMI is the designated successor of the CMM. [CMMI]

capture/playback tool: A type of test execution tool where inputs are recorded during manual testing in order to generate automated test scripts that can be executed later (i.e. replayed). These tools are often used to support automated regression testing.

capture/replay tool: See capture/playback tool.

CASE: Acronym for Computer Aided Software Engineering.

CAST: Acronym for Computer Aided Software Testing. See also test automation.

cause-effect graph: A graphical representation of inputs and/or stimuli (causes) with their associated outputs (effects), which can be used to design test cases.

cause-effect graphing: A black box test design technique in which test cases are designed from cause-effect graphs. [BS 7925/2]

cause-effect analysis: See cause/effect graphing.

cause-effect decision table: See decision table.

certification: The process of confirming that a component, system or person complies with its specified requirements, e.g. by passing an exam.

changeability: The capability of the software product to enable specified modifications to be implemented. [ISO 9126] See also maintainability.

checker: See reviewer.

Chow's coverage metrics: See N-switch coverage. [Chow]

classification tree method: A black box test design technique in which test cases, described by means of a classification tree, are designed to execute combinations of representatives of input and/or output domains. [Grochtmann]

code analyzer: See static code analyzer.

code coverage: An analysis method that determines which parts of the software have been executed (covered) by the test suite and which parts have not been executed, e.g. statement coverage, decision coverage or condition coverage.

code-based testing: See white box testing.

co-existence: The capability of the software product to co-exist with other independent software in a common environment sharing common resources. [ISO 9126] See portability testing.

commercial off-the-shelf software: See off-the-shelf software.

comparator: See test comparator.

compatibility testing: See interoperability testing.

complete testing: See exhaustive testing.

completion criteria: See exit criteria.

complexity: The degree to which a component or system has a design and/or internal structure that is difficult to understand, maintain and verify. See also cyclomatic complexity.

compliance: The capability of the software product to adhere to standards, conventions or regulations in laws and similar prescriptions. [ISO 9126]

compliance testing: The process of testing to determine the compliance of component or system.

component: A minimal software item that can be tested in isolation.

component integration testing: Testing performed to expose defects in the interfaces and interaction between integrated components.

component specification: A description of a component's function in terms of its output values for specified input values under specified conditions, and required non-functional behavior (e.g. resource-utilization).

component testing: The testing of individual software components. [After IEEE 610]

compound condition: Two or more single conditions joined by means of a logical operator (AND, OR or XOR), e.g. 'A>B AND C>1000'.

concrete test case: See low level test case.

concurrency testing: Testing to determine how the occurrence of two or more activities within the same interval of time, achieved either by interleaving the activities or by simultaneous execution, is handled by the component or system. [After IEEE 610]

condition: A logical expression that can be evaluated as True or False, e.g. $A > B$. See also test condition.

condition combination coverage: See multiple condition coverage.

condition combination testing: See multiple condition testing.

condition coverage: The percentage of condition outcomes that have been exercised by a test suite. 100% condition coverage requires each single condition in every decision statement to be tested as True and False.

condition determination coverage: The percentage of all single condition outcomes that independently affect a decision outcome that have been exercised by a test case suite. 100% condition determination coverage implies 100% decision condition coverage.

condition determination testing: A white box test design technique in which test cases are designed to execute single condition outcomes that independently affect a decision outcome.

condition testing: A white box test design technique in which test cases are designed to execute condition outcomes.

condition outcome: The evaluation of a condition to True or False.

confidence test: See smoke test.

configuration: The composition of a component or system as defined by the number, nature, and interconnections of its constituent parts.

configuration auditing: The function to check on the contents of libraries of configuration items, e.g. for standards compliance. [IEEE 610]

configuration control: An element of configuration management, consisting of the evaluation, co-ordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. [IEEE 610]

configuration identification: An element of configuration management, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation. [IEEE 610]

configuration item: An aggregation of hardware, software or both, that is designated for configuration management and treated as a single entity in the configuration management process. [IEEE 610]

configuration management: A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. [IEEE 610]

configuration testing: See portability testing.

confirmation testing: See re-testing.

conformance testing: See compliance testing.

consistency: The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a component or system. [IEEE 610]

control flow: An abstract representation of all possible sequences of events (paths) in the execution through a component or system.

control flow graph: See control flow.

control flow path: See path.

conversion testing: Testing of software used to convert data from existing systems for use in replacement systems.

COTS: Acronym for Commercial Off-The-Shelf software.

coverage: The degree, expressed as a percentage, to which a specified coverage item has been exercised by a test suite.

coverage analysis: Measurement of achieved coverage to a specified coverage item during test execution referring to predetermined criteria to determine whether additional testing is required and if so, which test cases are needed.

coverage item: An entity or property used as a basis for test coverage, e.g. equivalence partitions or code statements.

coverage tool: A tool that provides objective measures of what structural elements, e.g. statements, branches have been exercised by the test suite.

custom software: See bespoke software.

cyclomatic complexity: The number of independent paths through a program. Cyclomatic complexity is defined as: $L - N + 2P$, where

- L = the number of edges/links in a graph
 - N = the number of nodes in a graph
 - P = the number of disconnected parts of the graph (e.g. a calling graph and a subroutine).
- [After McCabe]

cyclomatic number: See cyclomatic complexity.

D

data definition: An executable statement where a variable is assigned a value.

data driven testing: A scripting technique that stores test input and expected results in a table or spreadsheet, so that a single control script can execute all of the tests in the table. Data driven testing is often used to support the application of test execution tools such as capture/playback tools. [Fewster and Graham] See also keyword driven testing.

data flow: An abstract representation of the sequence and possible changes of the state of data objects, where the state of an object is any of: creation, usage, or destruction. [Beizer]

data flow analysis: A form of static analysis based on the definition and usage of variables.

data flow coverage: The percentage of definition-use pairs that have been exercised by a test case suite.

data flow test: A white box test design technique in which test cases are designed to execute definition and use pairs of variables.

dead code: See unreachable code.

debugger: See debugging tool.

debugging: The process of finding, analyzing and removing the causes of failures in software.

debugging tool: A tool used by programmers to reproduce failures, investigate the state of programs and find the corresponding defect. Debuggers enable programmers to execute programs step by step, to halt a program at any program statement and to set and examine program variables.

decision: A program point at which the control flow has two or more alternative routes. A node with two or more links to separate branches.

decision condition coverage: The percentage of all condition outcomes and decision outcomes that have been exercised by a test suite. 100% decision condition coverage implies both 100% condition coverage and 100% decision coverage.

decision condition testing: A white box test design technique in which test cases are designed to execute condition outcomes and decision outcomes.

decision coverage: The percentage of decision outcomes that have been exercised by a test suite. 100% decision coverage implies both 100% branch coverage and 100% statement coverage.

decision table: A table showing combinations of inputs and/or stimuli (causes) with their associated outputs and/or actions (effects), which can be used to design test cases.

decision table testing: A black box test design techniques in which test cases are designed to execute the combinations of inputs and/or stimuli (causes) shown in a decision table. [Veenendaal]

decision testing: A white box test design technique in which test cases are designed to execute decision outcomes.

decision outcome: The result of a decision (which therefore determines the branches to be taken).

defect: A flaw in a component or system that can cause the component or system to fail to perform its required function, e.g. an incorrect statement or data definition. A defect, if encountered during execution, may cause a failure of the component or system.

defect density: The number of defects identified in a component or system divided by the size of the component or system (expressed in standard measurement terms, e.g. lines-of-code, number of classes or function points).

Defect Detection Percentage (DDP): the number of defects found by a test phase, divided by the number found by that test phase and any other means afterwards.

defect report: A document reporting on any flaw in a component or system that can cause the component or system to fail to perform its required function. [After IEEE 829]

defect tracking tool: See incident management tool.

defect management: The process of recognizing, investigating, taking action and disposing of defects. It involves recording defects, classifying them and identifying the impact. [After IEEE 1044]

defect management tool: See incident management tool.

defect masking: An occurrence in which one defect prevents the detection of another. [After IEEE 610]

definition-use pair: The association of the definition of a variable with the use of that variable. Variable uses include computational (e.g. multiplication) or to direct the execution of a path (“predicate” use).

deliverable: Any (work) product that must be delivered to someone other than the (work) product's author.

design-based testing: An approach to testing in which test cases are designed based on the architecture and/or detailed design of a component or system (e.g. tests of interfaces between components or systems).

desk checking: Testing of software or specification by manual simulation of its execution.

development testing: Formal or informal testing conducted during the implementation of a component or system, usually in the development environment by developers. [After IEEE 610]

deviation: See incident.

deviation report: See incident report.

dirty testing: See negative testing.

documentation testing: Testing the quality of the documentation, e.g. user guide or installation guide.

domain: The set from which valid input and/or output values can be selected.

driver: A software component or test tool that replaces a component that takes care of the control and/or the calling of a component or system. [After TMap]

dynamic analysis: The process of evaluating behavior, e.g. memory performance, CPU usage, of a system or component during execution. [After IEEE 610]

dynamic comparison: Comparison of actual and expected results, performed while the software is being executed, for example by a test execution tool.

dynamic testing: Testing that involves the execution of the software of a component or system.

E

efficiency: The capability of the software product to provide appropriate performance, relative to the amount of resources used under stated conditions. [ISO 9126]

efficiency testing: The process of testing to determine the efficiency of a software product.

elementary comparison testing: A black box test design technique in which test cases are designed to execute combinations of inputs using the concept of condition determination coverage. [TMap]

emulator: A device, computer program, or system that accepts the same inputs and produces the same outputs as a given system. [IEEE 610] See also simulator.

entry criteria: the set of generic and specific conditions for permitting a process to go forward with a defined task, e.g. test phase. The purpose of entry criteria is to prevent a task from starting which would entail more (wasted) effort compared to the effort needed to remove the failed entry criteria. [Gilb and Graham]

entry point: The first executable statement within a component.

equivalence class: See equivalence partition.

equivalence partition: A portion of an input or output domain for which the behavior of a component or system is assumed to be the same, based on the specification.

equivalence partition coverage: The percentage of equivalence partitions that have been exercised by a test suite.

equivalence partitioning: A black box test design technique in which test cases are designed to execute representatives from equivalence partitions. In principle test cases are designed to cover each partition at least once.

error: A human action that produces an incorrect result. [After IEEE 610]

error guessing: A test design technique where the experience of the tester is used to anticipate what defects might be present in the component or system under test as a result of errors made, and to design tests specifically to expose them.

error seeding: The process of intentionally adding known defects to those already in the component or system for the purpose of monitoring the rate of detection and removal, and estimating the number of remaining defects. [IEEE 610]

error tolerance: The ability of a system or component to continue normal operation despite the presence of erroneous inputs. [After IEEE 610].

evaluation: See testing.

exception handling: Behavior of a component or system in response to erroneous input, from either a human user or from another component or system, or to an internal failure.

executable statement: A statement which, when compiled, is translated into object code, and which will be executed procedurally when the program is running and may perform an action on data.

exercised: A program element is said to be exercised by a test case when the input value causes the execution of that element, such as a statement, decision, or other structural element.

exhaustive testing: A test approach in which the test suite comprises all combinations of input values and preconditions.

exit criteria: The set of generic and specific conditions, agreed upon with the stakeholders, for permitting a process to be officially completed. The purpose of exit criteria is to prevent a task from being considered completed when there are still outstanding parts of the task which have not been finished. Exit criteria are used by testing to report against and to plan when to stop testing. [After Gilb and Graham]

exit point: The last executable statement within a component.

expected outcome: See expected result.

expected result: The behavior predicted by the specification, or another source, of the component or system under specified conditions.

exploratory testing: Testing where the tester actively controls the design of the tests as those tests are performed and uses information gained while testing to design new and better tests. [Bach]

F

fail: A test is deemed to fail if its actual result does not match its expected result.

failure: Actual deviation of the component or system from its expected delivery, service or result. [After Fenton]

failure mode: The physical or functional manifestation of a failure. For example, a system in failure mode may be characterized by slow operation, incorrect outputs, or complete termination of execution.

Failure Mode and Effect Analysis (FMEA): A systematic approach to risk identification and analysis of identifying possible modes of failure and attempting to prevent their occurrence.

failure rate: The ratio of the number of failures of a given category to a given unit of measure, e.g. failures per unit of time, failures per number of transactions, failures per number of computer runs. [IEEE 610]

fault: See defect.

fault density: See defect density.

Fault Detection Percentage (FDP): See Defect Detection Percentage (DDP).

fault masking: See defect masking.

fault tolerance: The capability of the software product to maintain a specified level of performance in cases of software faults (defects) or of infringement of its specified interface. [ISO 9126] See also reliability.

fault tree analysis: A method used to analyze the causes of faults (defects).

feasible path: A path for which a set of input values and preconditions exists which causes it to be executed.

feature: An attribute of a component or system specified or implied by requirements documentation (for example reliability, usability or design constraints). [After IEEE 1008]

field testing: See beta testing.

finite state machine: A computational model consisting of a finite number of states and transitions between those states, possibly with accompanying actions. [IEEE 610]

finite state testing: See state transition testing.

formal review: A review characterized by documented procedures and requirements, e.g. inspection.

frozen test basis: A test basis document that can only be amended by a formal change control process. See also baseline.

Function Point Analysis (FPA): Method aiming to measure the size of the functionality of an information system. The measurement is independent of the technology. This measurement may be used as a basis for the measurement of productivity, the estimation of the needed resources, and project control.

functional integration: An integration approach that combines the components or systems for the purpose of getting a basic functionality working early. See also integration testing.

functional requirement: A requirement that specifies a function that a component or system must perform. [IEEE 610]

functional test design technique: Documented procedure to derive and select test cases based on an analysis of the specification of the functionality of a component or system without reference to its internal structure. See also black box test design technique.

functional testing: Testing based on an analysis of the specification of the functionality of a component or system. See also black box testing.

functionality: The capability of the software product to provide functions which meet stated and implied needs when the software is used under specified conditions. [ISO 9126]

functionality testing: The process of testing to determine the functionality of a software product.

G

glass box testing: See white box testing.

H

heuristic evaluation: A static usability test technique to determine the compliance of a user interface with recognized usability principles (the so-called “heuristics”).

high level test case: A test case without concrete (implementation level) values for input data and expected results.

horizontal traceability: The tracing of requirements for a test level through the layers of test documentation (e.g. test plan, test design specification, test case specification and test procedure specification).

I

impact analysis: The assessment of change to the layers of development documentation, test documentation and components, in order to implement a given change to specified requirements.

incremental development model: A development life cycle where a project is broken into a series of increments, each of which delivers a portion of the functionality in the overall project requirements. The requirements are prioritized and delivered in priority order in the appropriate increment. In some (but not all) versions of this life cycle model, each subproject follows a ‘mini V-model’ with its own design, coding and testing phases.

incremental testing: Testing where components or systems are integrated and tested one or some at a time, until all the components or systems are integrated and tested.

incident: Any event occurring during testing that requires investigation. [After IEEE 1008]

incident management: The process of recognizing, investigating, taking action and disposing of incidents. It involves recording incidents, classifying them and identifying the impact. [After IEEE 1044]

incident management tool: A tool that facilitates the recording and status tracking of incidents found during testing. They often have workflow-oriented facilities to track and control the allocation, correction and re-testing of incidents and provide reporting facilities.

incident report: A document reporting on any event that occurs during the testing which requires investigation. [After IEEE 829]

independence: Separation of responsibilities, which encourages the accomplishment of objective testing. [After DO-178b]

infeasible path: A path that cannot be exercised by any set of possible input values.

informal review: A review not based on a formal (documented) procedure.

input: A variable (whether stored within a component or outside) that is read by a component.

input domain: The set from which valid input values can be selected.. See also domain.

input value: An instance of an input. See also input.

inspection: A type of review that relies on visual examination of documents to detect defects, e.g. violations of development standards and non-conformance to higher level documentation. The most formal review technique and therefore always based on a documented procedure. [After IEEE 610, IEEE 1028]

inspection leader: See moderator.

inspector: See reviewer.

installability: The capability of the software product to be installed in a specified environment [ISO 9126]. See also portability.

installability testing: The process of testing the installability of a software product. See also portability testing.

installation guide: Supplied instructions on any suitable media, which guides the installer through the installation process. This may be a manual guide, step-by-step procedure, installation wizard, or any other similar process description.

installation wizard: Supplied software on any suitable media, which leads the installer through the installation process. It normally runs the installation process, provides feedback on installation results, and prompts for options.

instrumentation: The insertion of additional code into the program in order to collect information about program behavior during execution.

instrumenter: A software tool used to carry out instrumentation.

intake test: A special instance of a smoke test to decide if the component or system is ready for detailed and further testing. An intake test is typically carried out at the start of the test execution phase.

integration: The process of combining components or systems into larger assemblies.

integration testing: Testing performed to expose defects in the interfaces and in the interactions between integrated components or systems. See also component integration testing, system integration testing.

integration testing in the large: See system integration testing.

integration testing in the small: See component integration testing.

interface testing: An integration test type that is concerned with testing the interfaces between components or systems.

interoperability: The capability of the software product to interact with one or more specified components or systems. [After ISO 9126] See also functionality.

interoperability testing: The process of testing to determine the interoperability of a software product. See also functionality testing.

invalid testing: Testing using input values that should be rejected by the component or system. See also error tolerance.

isolation testing: Testing of individual components in isolation from surrounding components, with surrounding components being simulated by stubs and drivers, if needed.

item transmittal report: See release note.

K

key performance indicator: See performance indicator.

keyword driven testing: A scripting technique that uses data files to contain not only test data and expected results, but also keywords related to the application being tested. The keywords are interpreted by special supporting scripts that are called by the control script for the test. See also data driven testing.

L

LCSAJ: A Linear Code Sequence And Jump, consisting of the following three items (conventionally identified by line numbers in a source code listing): the start of the linear sequence of executable statements, the end of the linear sequence, and the target line to which control flow is transferred at the end of the linear sequence.

LCSAJ coverage: The percentage of LCSAJs of a component that have been exercised by a test suite. 100% LCSAJ coverage implies 100% decision coverage.

LCSAJ testing: A white box test design technique in which test cases are designed to execute LCSAJs.

learnability: The capability of the software product to enable the user to learn its application. [ISO 9126] See also usability.

link testing: See component integration testing.

load test: A test type concerned with measuring the behavior of a component or system with increasing load, e.g. number of parallel users and/or numbers of transactions to determine what load can be handled by the component or system.

logic-coverage testing: See white box testing. [Myers]

logic-driven testing: See white box testing.

logical test case: See high level test case.

low level test case: A test case with concrete (implementation level) values for input data and expected results.

M

maintenance: Modification of a software product after delivery to correct defects, to improve performance or other attributes, or to adapt the product to a modified environment. [IEEE 1219]

maintenance testing: Testing the changes to an operational system or the impact of a changed environment to an operational system.

maintainability: The ease with which a software product can be modified to correct defects, modified to meet new requirements, modified to make future maintenance easier, or adapted to a changed environment. [ISO 9126]

maintainability testing: The process of testing to determine the maintainability of a software product.

management review: A systematic evaluation of software acquisition, supply, development, operation, or maintenance process, performed by or on behalf of management that monitors progress, determines the status of plans and schedules, confirms requirements and

their system allocation, or evaluates the effectiveness of management approaches to achieve fitness for purpose. [After IEEE 610, IEEE 1028]

maturity: (1) The capability of an organization with respect to the effectiveness and efficiency of its processes and work practices. See also Capability Maturity Model, Test Maturity Model. (2) The capability of the software product to avoid failure as a result of defects in the software. [ISO 9126] See also reliability.

master test plan: See project test plan.

measure: The number or category assigned to an attribute of an entity by making a measurement [ISO 14598].

measurement: The process of assigning a number or category to an entity to describe an attribute of that entity. [ISO 14598]

measurement scale: A scale that constrains the type of data analysis that can be performed on it. [ISO 14598]

memory leak: A defect in a program's dynamic store allocation logic that causes it to fail to reclaim memory after it has finished using it, eventually causing the program to fail due to lack of memory.

metric: A measurement scale and the method used for measurement. [ISO 14598]

migration testing: See conversion testing.

milestone: A point in time in a project at which defined (intermediate) deliverables and results should be ready.

mistake: See error.

moderator: The leader and main person responsible for an inspection or other review process.

modified condition decision coverage: See condition determination coverage.

modified condition decision testing: See condition determination coverage testing.

modified multiple condition coverage: See condition determination coverage.

modified multiple condition testing: See condition determination coverage testing.

module: See component.

module testing: See component testing.

monitor: A software tool or hardware device that run concurrently with the component or system under test and supervises, records and/or analyses the behavior of the component or system. [After IEEE 610]

multiple condition: See compound condition.

multiple condition coverage: The percentage of combinations of all single condition outcomes within one statement that have been exercised by a test suite. 100% multiple condition coverage implies 100% condition determination coverage.

multiple condition testing: A white box test design technique in which test cases are designed to execute combinations of single condition outcomes (within one statement).

mutation analysis: A method to determine test suite thoroughness by measuring the extent to which a test suite can discriminate the program from slight variants (mutants) of the program.

N

N-switch coverage: The percentage of sequences of N+1 transitions that have been exercised by a test suite. [Chow]

N-switch testing: A form of state transition testing in which test cases are designed to execute all valid sequences of N+1 transitions. [Chow] See also state transition testing.

negative testing: Tests aimed at showing that a component or system does not work. Negative testing is related to the testers' attitude rather than a specific test approach or test design technique. [After Beizer].

non-conformity: Non fulfillment of a specified requirement. [ISO 9000]

non-functional requirement: A requirement that does not relate to functionality, but to attributes of such as reliability, efficiency, usability, maintainability and portability.

non-functional testing: Testing the attributes of a component or system that do not relate to functionality, e.g. reliability, efficiency, usability, maintainability and portability.

non-functional test design techniques: Methods used to design or select tests for non-functional testing.

O

off-the-shelf software: A software product that is developed for the general market, i.e. for a large number of customers, and that is delivered to many customers in identical format.

operability: The capability of the software product to enable the user to operate and control it. [ISO 9126] See also usability.

operational environment: Hardware and software products installed at users' or customers' sites where the component or system under test will be used. The software may include operating systems, database management systems, and other applications.

operational profile testing: Statistical testing using a model of system operations (short duration tasks) and their probability of typical use. [Musa]

operational testing: Testing conducted to evaluate a component or system in its operational environment. [IEEE 610]

oracle: See test oracle.

outcome: See result.

output: A variable (whether stored within a component or outside) that is written by a component.

output domain: The set from which valid output values can be selected. See also domain.

output value: An instance of an output. See also output.

P

pair programming: A software development approach whereby lines of code (production and/or test) of a component are written by two programmers sitting at a single computer. This implicitly means ongoing real-time code reviews are performed.

pair testing: Two testers work together to find defects. Typically, they share one computer and trade control of it while testing.

partition testing: See equivalence partitioning. [Beizer]

pass: A test is deemed to pass if its actual result matches its expected result.

pass/fail criteria: Decision rules used to determine whether a test item (function) or feature has passed or failed a test. [IEEE 829]

path: A sequence of events, e.g. executable statements, of a component or system from an entry point to an exit point.

path coverage: The percentage of paths that have been exercised by a test suite. 100% path coverage implies 100% LCSAJ coverage.

path sensitizing: Choosing a set of input values to force the execution of a given path.

path testing: A white box test design technique in which test cases are designed to execute paths.

peer review: See technical review.

performance: The degree to which a system or component accomplishes its designated functions within given constraints regarding processing time and throughput rate. [After IEEE 610] See efficiency.

performance indicator: A high level metric of effectiveness and/or efficiency used to guide and control progressive development, e.g. Defect Detection Percentage (DDP) for testing. [CMMI]

performance testing: The process of testing to determine the performance of a software product. See efficiency testing.

performance testing tool: A tool to support performance testing and that usually has two main facilities: load generation and test transaction measurement. Load generation can simulate either multiple users or high volumes of input data. During execution, response time measurements are taken from selected transactions and these are logged. Performance testing tools normally provide reports based on test logs and graphs of load against response times.

phase test plan: A test plan that typically addresses one test level.

portability: The ease with which the software product can be transferred from one hardware or software environment to another. [ISO 9126]

portability testing: The process of testing to determine the portability of a software product.

postcondition: Environmental and state conditions that must be fulfilled after the execution of a test or test procedure.

post-execution comparison: Comparison of actual and expected results, performed after the software has finished running.

precondition: Environmental and state conditions that must be fulfilled before the component or system can be executed with a particular test or test procedure.

predicted outcome: See expected result.

pretest: See intake test.

priority: The level of (business) importance assigned to an item, e.g. defect.

process cycle test: A black box test design technique in which test cases are designed to execute business procedures and processes. [TMap]

problem: See defect.

problem management: See defect management.

problem report: See defect report.

process: A set of interrelated activities, which transform inputs into outputs. [ISO 12207]

project: A project is a unique set of coordinated and controlled activities with start and finish dates undertaken an objective conforming to specific requirements, including the constraints of time, cost and resources. [ISO 9000]

program instrumenter: See instrumenter.

program testing: See component testing.

project test plan: A test plan that typically addresses multiple test levels.

pseudo-random: A series which appears to be random but is in fact generated according to some prearranged sequence.

Q

quality: The degree to which a component, system or process meets specified requirements and/or user/customer needs and expectations. [After IEEE 610]

quality assurance: Part of quality management focused on providing confidence that quality requirements will be fulfilled. [ISO 9000]

quality attribute: A feature or characteristic that affects an item's quality. [IEEE 610]

quality characteristic: See quality attribute.

quality management: Coordinated activities to direct and control an organization with regard to quality. Direction and control with regard to quality generally includes the establishment of the quality policy and quality objectives, quality planning, quality control, quality assurance and quality improvement. [ISO 9000]

R

random testing: A black box test design technique where test cases are selected, possibly using a pseudo-random generation algorithm, to match an operational profile. This technique can be used for testing non-functional attributes such as reliability and performance.

recorder: See scribe.

record/playback tool: See capture/playback tool.

recoverability: The capability of the software product to re-establish a specified level of performance and recover the data directly affected in case of failure. [ISO 9126] See also reliability.

recoverability testing: The process of testing to determine the recoverability of a software product. See also reliability testing.

recovery testing: See recoverability testing.

regression testing: Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made. It is performed when the software or its environment is changed.

release note: A document identifying test items, their configuration, current status and other delivery information delivered by development to testing, and possibly other stakeholders, at the start of a test execution phase. [After IEEE 829]

reliability: The ability of the software product to perform its required functions under stated conditions for a specified period of time, or for a specified number of operations. [ISO 9126]

reliability testing: The process of testing to determine the reliability of a software product.

replaceability: The capability of the software product to be used in place of another specified software product for the same purpose in the same environment. [ISO 9126] See also portability.

requirement: A condition or capability needed by a user to solve a problem or achieve an objective that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed document. [After IEEE 610]

requirements-based testing: An approach to testing in which test cases are designed based on test objectives and test conditions derived from requirements, e.g. tests that exercise specific functions or probe non-functional attributes such as reliability or usability.

requirements management tool: A tool that supports the recording of requirements, requirements attributes (e.g. priority, knowledge responsible) and annotation, and facilitates traceability through layers of requirements and requirements change management. Some requirements management tools also provide facilities for static analysis, such as consistency checking and violations to pre-defined requirements rules.

requirements phase: The period of time in the software life cycle during which the requirements for a software product are defined and documented. [IEEE 610]

resource utilization: The capability of the software product to use appropriate amounts and types of resources, for example the amounts of main and secondary memory used by the program and the sizes of required temporary or overflow files, when the software performs its function under stated conditions. [After ISO 9126] See also efficiency.

resource utilization testing: The process of testing to determine the resource-utilization of a software product.

result: The consequence/outcome of the execution of a test. It includes outputs to screens, changes to data, reports, and communication messages sent out. See also actual result, expected result.

resumption criteria: The testing activities that must be repeated when testing is re-started after a suspension. [After IEEE 829]

re-testing: Testing that runs test cases that failed the last time they were run, in order to verify the success of corrective actions.

review: An evaluation of a product or project status to ascertain discrepancies from planned results and to recommend improvements. Examples include management review, informal review, technical review, inspection, and walkthrough. [After IEEE 1028]

reviewer: The person involved in the review who shall identify and describe anomalies in the product or project under review. Reviewers can be chosen to represent different viewpoints and roles in the review process.

risk: A factor that could result in future negative consequences; usually expressed as impact and likelihood.

risk analysis: The process of assessing identified risks to estimate their impact and probability of occurrence (likelihood).

risk-based testing: Testing oriented towards exploring and providing information about product risks. [After Gerrard]

risk control: The process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.

risk identification: The process of identifying risks using techniques such as brainstorming, checklists and failure history.

risk management: Systematic application of procedures and practices to the tasks of identifying, analyzing, prioritizing, and controlling risk.

risk mitigation: See risk control.

robustness: The degree to which a component or system can function correctly in the presence of invalid inputs or stressful environmental conditions. [IEEE 610] See also error-tolerance, fault-tolerance.

root cause: An underlying factor that caused a non-conformance and possibly should be permanently eliminated through process improvement.

S

safety: The capability of the software product to achieve acceptable levels of risk of harm to people, business, software, property or the environment in a specified context of use. [ISO 9126]

safety testing: The process of testing to determine the safety of a software product.

sanity test: See smoke test.

scalability: The capability of the software product to be upgraded to accommodate increased loads. [After Gerrard]

scalability testing: Testing to determine the scalability of the software product.

scenario testing: See use case testing.

scribe: The person who has to record each defect mentioned and any suggestions for improvement during a review meeting, on a logging form. The scribe has to make ensure that the logging form is readable and understandable.

scripting language: A programming language in which executable test scripts are written, used by a test execution tool (e.g. a capture/replay tool).

security: Attributes of software products that bear on its ability to prevent unauthorized access, whether accidental or deliberate, to programs and data. [ISO 9126]

security testing: Testing to determine the security of the software product.

serviceability testing: See maintainability testing.

severity: The degree of impact that a defect has on the development or operation of a component or system. [After IEEE 610]

simulation: The representation of selected behavioral characteristics of one physical or abstract system by another system. [ISO 2382/1]

simulator: A device, computer program or system used during testing, which behaves or operates like a given system when provided with a set of controlled inputs. [After IEEE 610, DO178b] See also emulator.

smoke test: A subset of all defined/planned test cases that cover the main functionality of a component or system, to ascertaining that the most crucial functions of a program work, but not bothering with finer details. A daily build and smoke test is among industry best practices. See also intake test.

software quality: The totality of functionality and features of a software product that bear on its ability to satisfy stated or implied needs. [After ISO 9126]

software quality characteristic: See quality attribute.

software feature: See feature.

software test incident: See incident.

software test incident report: See incident report.

source statement: See statement.

specification: A document that specifies, ideally in a complete, precise and verifiable manner, the requirements, design, behavior, or other characteristics of a component or system, and, often, the procedures for determining whether these provisions have been satisfied. [After IEEE 610]

specification-based testing: See black box testing.

specification-based test design technique: See black box test design technique.

specified input: An input for which the specification predicts a result.

stability: The capability of the software product to avoid unexpected effects from modifications in the software. [ISO 9126] See also maintainability.

standard software: See off-the-shelf software.

standards testing: See compliance testing.

state diagram: A diagram that depicts the states that a component or system can assume, and shows the events or circumstances that cause and/or result from a change from one state to another. [IEEE 610]

state table: A grid showing the resulting transitions for each state combined with each possible event, showing both valid and invalid transitions.

state transition: A transition between two states of a component or system.

state transition testing: A black box test design technique in which test cases are designed to execute valid and invalid state transitions. See also N-switch testing.

statement: An entity in a programming language, which is typically the smallest indivisible unit of execution.

statement coverage: The percentage of executable statements that have been exercised by a test suite.

statement testing: A white box test design technique in which test cases are designed to execute statements.

static analysis: Analysis of software artifacts, e.g. requirements or code, carried out without execution of these software artifacts.

static analyzer: A tool that carries out static analysis.

static code analysis: Analysis of program source code carried out without execution of that software.

static code analyzer: A tool that carries out static code analysis. The tool checks source code, for certain properties such as conformance to coding standards, quality metrics or data flow anomalies.

static testing: Testing of a component or system at specification or implementation level without execution of that software, e.g. reviews or static code analysis.

statistical testing: A test design technique in which a model of the statistical distribution of the input is used to construct representative test cases. See also operational profile testing.

status accounting: An element of configuration management, consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of the approved changes. [IEEE 610]

storage: See resource utilization.

storage testing: See resource utilization testing.

stress testing: Testing conducted to evaluate a system or component at or beyond the limits of its specified requirements. [IEEE 610]

structural coverage: Coverage measures based on the internal structure of the component.

structural test design technique: See white box test design technique.

structural testing: See white box testing.

structured walkthrough: See walkthrough.

stub: A skeletal or special-purpose implementation of a software component, used to develop or test a component that calls or is otherwise dependent on it. It replaces a called component. [After IEEE 610]

subpath: A sequence of executable statements within a component.

suspension criteria: The criteria used to (temporarily) stop all or a portion of the testing activities on the test items. [After IEEE 829]

suitability: The capability of the software product to provide an appropriate set of functions for specified tasks and user objectives. [ISO 9126] See also functionality.

Software Usability Measurement Inventory (SUMI): A questionnaire based usability test technique to evaluate the usability, e.g. user-satisfaction, of a component or system. [Veenendaal]

syntax testing: A black box test design technique in which test cases are designed based upon the definition of the input domain and/or output domain.

system: A collection of components organized to accomplish a specific function or set of functions. [IEEE 610]

system integration testing: Testing the integration of systems and packages; testing interfaces to external organizations (e.g. Electronic Data Interchange, Internet).

system testing: The process of testing an integrated system to verify that it meets specified requirements. [Hetzel]

T

technical review: A peer group discussion activity that focuses on achieving consensus on the technical approach to be taken. A technical review is also known as a peer review. [Gilb and Graham, IEEE 1028]

test: A set of one or more test cases [IEEE 829]

test approach: The implementation of the test strategy for a specific project. It typically includes the decisions made that follow based on the (test) project's goal and the risk assessment carried out, starting points regarding the test process, the test design techniques to be applied, exit criteria and test types to be performed.

test automation: The use of software to perform or support test activities, e.g. test management, test design, test execution and results checking.

test basis: All documents from which the requirements of a component or system can be inferred. The documentation on which the test cases are based. If a document can be amended only by way of formal amendment procedure, then the test basis is called a frozen test basis. [After TMap]

test bed: See test environment.

test case: A set of input values, execution preconditions, expected results and execution postconditions, developed for a particular objective or test condition, such as to exercise a particular program path or to verify compliance with a specific requirement. [After IEEE 610]

test case design technique: See test design technique.

test case specification: A document specifying a set of test cases (objective, inputs, test actions, expected results, and execution preconditions) for a test item. [After IEEE 829]

test case suite: See test suite.

test charter: A statement of test objectives, and possibly test ideas. Test charters are amongst other used in exploratory testing. See also exploratory testing.

test comparator: A test tool to perform automated test comparison.

test comparison: The process of identifying differences between the actual results produced by the component or system under test and the expected results for a test. Test comparison can be performed during test execution (dynamic comparison) or after test execution.

test completion criterion: See exit criteria.

test condition: An item or event of a component or system that could be verified by one or more test cases, e.g. a function, transaction, quality attribute, or structural element.

test coverage: See coverage.

test data: Data that exists (for example, in a database) before a test is executed, and that affects or is affected by the component or system under test.

test data preparation tool: A type of test tool that enables data to be selected from existing databases or created, generated, manipulated and edited for use in testing.

test design: See test design specification.

test design specification: A document specifying the test conditions (coverage items) for a test item, the detailed test approach and identifying the associated high level test cases. [After IEEE 829]

test design tool: A tool that support the test design activity by generating test inputs from a specification that may be held in a CASE tool repository, e.g. requirements management tool, or from specified test conditions held in the tool itself.

test design technique: A method used to derive or select test cases.

test driver: See driver.

test environment: An environment containing hardware, instrumentation, simulators, software tools, and other support elements needed to conduct a test. [After IEEE 610]

test evaluation report: A document produced at the end of the test process summarizing all testing activities and results. It also contains an evaluation of the test process and lessons learned.

test execution: The process of running a test by the component or system under test, producing actual result(s).

test execution automation: The use of software, e.g. capture/playback tools, to control the execution of tests, the comparison of actual results to expected results, the setting up of test preconditions, and other test control and reporting functions.

test execution phase: The period of time in a software development life cycle during which the components of a software product are executed, and the software product is evaluated to determine whether or not requirements have been satisfied. [IEEE 610]

test execution schedule: A scheme for the execution of test procedures. The test procedures are included in the test execution schedule in their context and in the order in which they are to be executed.

test execution technique: The method used to perform the actual test execution, either manually or automated.

test execution tool: A type of test tool that is able to execute other software using an automated test script, e.g. capture/playback. [Fewster and Graham]

test fail: See fail.

test generator: See test data preparation tool.

test harness: A test environment comprised of stubs and drivers needed to conduct a test.

test incident: See incident.

test incident report: See incident report.

test infrastructure: The organizational artifacts needed to perform testing, consisting of test environments, test tools, office environment and procedures.

test item: The individual element to be tested. There usually is one test object and many test items. See also test object.

test item transmittal report: See release note.

test level: A group of test activities that are organized and managed together. A test level is linked to the responsibilities in a project. Examples of test levels are component test, integration test, system test and acceptance test. [After TMap]

test log: A chronological record of relevant details about the execution of tests. [IEEE 829]

test logging: The process of recording information about tests executed into a test log.

test manager: The person responsible for testing and evaluating a test object. The individual, who directs, controls, administers plans and regulates the evaluation of a test object.

test management: The planning, estimating, monitoring and control of test activities, typically carried out by a test manager.

Test Maturity Model (TMM): A five level staged framework for test process improvement, related to the Capability Maturity Model (CMM) that describes the key elements of an effective test process.

Test Process Improvement (TPI): A continuous framework for test process improvement that describes the key elements of an effective test process, especially targeted at system testing and acceptance testing.

test object: The component or system to be tested. See also test item.

test objective: A reason or purpose for designing and executing a test.

test oracle: A source to determine expected results to compare with the actual result of the software under test. An oracle may be the existing system (for a benchmark), a user manual, or an individual's specialized knowledge, but should not be the code. [After Adrion]

test outcome: See result.

test pass: See pass.

test performance indicator: A metric, in general high level, indicating to what extent a certain target value or criterion is met. Often related to test process improvement objectives, e.g. Defect Detection Percentage (DDP).

test phase: A distinct set of test activities collected into a manageable phase of a project, e.g. the execution activities of a test level. [After Gerrard]

test plan: A document describing the scope, approach, resources and schedule of intended test activities. It identifies amongst others test items, the features to be tested, the testing tasks, who will do each task, degree of tester independence, the test environment, the test design techniques and test measurement techniques to be used, and the rationale for their choice, and any risks requiring contingency planning. It is a record of the test planning process [After IEEE 829]

test planning: The activity of establishing or updating a test plan.

test policy: A high level document describing the principles, approach and major objectives of the organization regarding testing.

test point analysis (TPA): A formula based test estimation method based on function point analysis. [TMap]

test procedure: See test procedure specification.

test procedure specification: A document specifying a sequence of actions for the execution of a test. Also known as test script or manual test script. [After IEEE 829]

test process: The fundamental test process comprises planning, specification, execution, recording and checking for completion. [BS 7925/2]

test record: See test log.

test recording: See test logging.

test repeatability: An attribute of a test indicating whether the same results are produced each time the test is executed.

test report: See test summary report.

test run: Execution of a test on a specific version of the test object.

test run log: See test log.

test result: See result.

test situation: See test condition.

test script: Commonly used to refer to a test procedure specification, especially an automated one.

test specification: A document that consists of a test design specification, test case specification and/or test procedure specification.

test stage: See test level.

test strategy: A high-level document defining the test levels to be performed and the testing within those levels for a programme (one or more projects).

test suite: A set of several test cases for a component or system under test, where the post condition of one test is often used as the precondition for the next one.

test summary report: A document summarizing testing activities and results. It also contains an evaluation of the corresponding test items against exit criteria. [After IEEE 829]

test target: A set of exit criteria.

test tool: A software product that supports one or more test activities, such as planning and control, specification, building initial files and data, test execution and test analysis. [TMap] See also CAST.

test type: A group of test activities aimed at testing a component or system regarding one or more interrelated quality attributes. A test type is focused on a specific test objective, i.e. reliability test, usability test, regression test etc., and may take place on one or more test levels or test phases. [After TMap]

testability: The capability of the software product to enable modified software to be tested. [ISO 9126] See also maintainability.

testability review: A detailed check of the test basis to determine whether the test basis is at an adequate quality level to act as an input document for the test process. [After TMap]

testable requirements: The degree to which a requirement is stated in terms that permit establishment of test designs (and subsequently test cases) and execution of tests to determine whether the requirements have been met. [After IEEE 610]

tester: A technically skilled professional who is involved in the testing of a component or system.

testing: The process consisting of all life cycle activities, both static and dynamic, concerned with planning, preparation and evaluation of software products and related work products to determine that they satisfy specified requirements, to demonstrate that they are fit for purpose and to detect defects.

testware: Artifacts produced during the test process required to plan, design, and execute tests, such as documentation, scripts, inputs, expected results, set-up and clear-up procedures, files, databases, environment, and any additional software or utilities used in testing. [After Fewster and Graham]

thread testing: A version of component integration testing where the progressive integration of components follows the implementation of subsets of the requirements, as opposed to the integration of components by levels of a hierarchy.

time behavior: See performance.

traceability: The ability to identify related items in documentation and software, such as requirements with associated tests. See also horizontal traceability, vertical traceability.

top-down testing: An incremental approach to integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs. Tested components are then used to test lower level components. The process is repeated until the lowest level components have been tested.

U

understandability: The capability of the software product to enable the user to understand whether the software is suitable, and how it can be used for particular tasks and conditions of use. [ISO 9126] See also usability.

unit testing: See component testing.

unreachable code: Code that cannot be reached and therefore is impossible to execute.

usability: The capability of the software to be understood, learned, used and attractive to the user when used under specified conditions. [ISO 9126]

usability testing: Testing to determine the extent to which the software product is understood, easy to learn, easy to operate and attractive to the users under specified conditions. [After ISO 9126]

use case testing: A black box test design technique in which test cases are designed to execute user scenarios.

user acceptance testing: See acceptance testing.

user scenario testing: See use case testing.

user test: A test whereby real-life users are involved to evaluate the usability of a component or system.

V

V-model: A framework to describe the software development life cycle activities from requirements specification to maintenance. The V-model illustrates how testing activities can be integrated into each phase of the software development life cycle.

validation: Confirmation by examination and through provision of objective evidence that the requirements for a specific intended use or application have been fulfilled. [ISO 9000]

variable: An element of storage in a computer that is accessible by a software program by referring to it by a name.

verification: Confirmation by examination and through the provision of objective evidence that specified requirements have been fulfilled. [ISO 9000]

vertical traceability: The tracing of requirements through the layers of development documentation to components.

volume testing: Testing where the system is subjected to large volumes of data. See also resource-utilization testing.

W

walkthrough: A step-by-step presentation by the author of a document in order to gather information and to establish a common understanding of its content. [Freedman and Weinberg, IEEE 1028]

white box test design technique: Documented procedure to derive and select test cases based on an analysis of the internal structure of a component or system.

white box testing: Testing based on an analysis of the internal structure of the component or system.

Wide Band Delphi: An expert based test estimation technique that aims at making an accurate estimation using the collective wisdom of the team members.

Annex A (Informative)

Index of sources; the following non-normative sources were used in constructing this glossary:

- [Abbott] J. Abbot (1986), *Software Testing Techniques*, NCC Publications.
- [Adrion] W. Adrion, M. Branstad and J. Cherniabsky (1982), Validation, Verification and Testing of Computer Software, in: *Computing Surveys*, Vol. 14, No 2, June 1982.
- [Bach] J. Bach (2004), Exploratory Testing, in: E. van Veenendaal, *The Testing Practitioner – 2nd edition*, UTN Publishing, ISBN 90-72194-65-9.
- [Beizer] B. Beizer (1990), *Software Testing Techniques*, van Nostrand Reinhold, ISBN 0-442-20672-0
- [Chow] T. Chow (1978), Testing Software Design Modelled by Finite-Sate Machines, in: *IEEE Transactions on Software Engineering*, Vol. 4, No 3, May 1978.
- [CMM] M. Paulk, C. Weber, B. Curtis and M.B. Chrissis (1995), *The Capability Maturity Model, Guidelines for Improving the Software Process*, Addison-Wesley, ISBN 0-201-54664-7
- [CMMI] M.B. Chrissis, M. Konrad and S. Shrum (2004), *CMMI, Guidelines for Process Integration and Product Improvement*, Addison Wesley, ISBN 0-321-15496-7
- [Fenton] N. Fenton (1991), *Software Metrics: a Rigorous Approach*, Chapman & Hall, London.
- [Fewster and Graham] M. Fewster and D. Graham (1999), *Software Test Automation, Effective use of test execution tools*, Addison-Wesley, ISBN 0-201-33140-3.
- [Freedman and Weinberg] D. Freedman and G. Weinberg (1990), *Walkthroughs, Inspections, and Technical Reviews*, Dorset House Publishing, ISBN 0-932633-19-6.
- [Gerrard] P. Gerrard and N. Thompson (2002), *Risk-Based E-Business Testing*, Artech House Publishers, ISBN 1-58053-314-0.
- [Gilb and Graham] T. Gilb and D. Graham (1993), *Software Inspection*, Addison-Wesley, ISBN 0-201-63181-4.
- [Grochtmann] M. Grochtmann (1994), Test Case Design Using Classification Trees, in: *Conference Proceedings STAR 1994*.
- [Hetzel] W. Hetzel (1988), *The complete guide to software testing*, 2nd edition, QED Information Sciences, ISBN 0-89435-242-3.
- [McCabe] T. McCabe (1976), A complexity measure, in: *IEEE Transactions on Software Engineering*, Vol. 2, pp. 308-320.
- [Musa] J. Musa (1998), *Software Reliability Engineering Testing*, McGraw-Hill Education, ISBN 0-07913-271-5.
- [Myers] G. Myers (1979), *The Art of Software Testing*, Wiley, ISBN 0-471-04328-1.
- [TMap] M. Pol, R. Teunissen, E. van Veenendaal (2002), *Software Testing, A guide to the TMap Approach*, Addison Wesley, ISBN 0-201-745712.
- [Veenendaal] E.P.W.M. van Veenendaal (2004), *The Testing Practitioner – 2nd edition*, UTN Publishing, ISBN 90-72194-65-9.

Annex B (Method of commenting on this glossary)

Comments are invited on this document so that the glossary can be further improved to satisfy the needs of the testing community.

When making a comment, be sure to include the following information:

- Your name and contact details;
- The version number of the glossary (currently 1.0);
- Exact part of the glossary;
- Supporting information, such as the reason for a proposed change, or the reference to the use of a term.

You can submit comments in a variety of ways, which in order of preference are as follows:

1. By E-mail to eve@improveqs.nl;
2. By post to Improve Quality Services BV, attn. Mr. E. van Veenendaal,
Waalresweg 39, 5554 HA, Valkenswaard, The Netherlands;
3. By FAX to +31 40 20 21450, marked for the attention of Erik van Veenendaal.