
Information technology — System and software integrity levels

Technologies de l'information — Niveaux d'intégrité du système et du logiciel



Contents		Page
1	Scope	1
2	Normative references	1
3	Definitions	2
4	Symbols and abbreviations.....	3
5	Software integrity levels framework	3
	5.1 How to use this International Standard	3
	5.2 Overview	3
6	System integrity level determination	6
	6.1 Risk analysis	6
	6.2 Risk evaluation.....	8
	6.3 System integrity level assignment.....	8
7	Software integrity level determination	8
	7.1 Assumptions in software integrity level determination	9
	7.2 Reduction of software integrity level	9
	7.3 Reducing the software integrity level of software whose failure can result in a threat.....	10
	7.4 Reducing the software integrity level of software whose failure may result in lack of provision of mitigating functions	10
8	Software integrity requirements determination	11
	8.1 Degree of confidence.....	11
	8.2 Methods of achieving degrees of confidence in software	11
	8.3 Association of degree of confidence in software with integrity level	11

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 15026 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software engineering*.

Information technology — System and software integrity levels

1 Scope

This International Standard introduces the concepts of software integrity levels and software integrity requirements. It defines the concepts associated with integrity levels, defines the processes for determining integrity levels and software integrity requirements, and places requirements on each process. This International Standard does not prescribe a specific set of integrity levels or software integrity requirements. These must be established either on a project by project basis, or for a specific sector and/or country. This International Standard is applicable to software only. The system integrity level and the integrity levels of the non-software components are only required in this International Standard to determine the integrity levels of the software components.

This International Standard is intended for use by developers, users, procurers, and assessors of software products or systems containing software for the administrative and technical support of those products and systems.

A software integrity level denotes a range of values of a software property necessary to maintain system risks within tolerable limits. For software that performs a mitigating function, the property is the reliability with which the software must perform the mitigating function. For software whose failure can lead to a system threat, the property is the limit on the frequency or probability of that failure.

Software integrity requirements are requirements that must be met by the software engineering process used to develop the software, requirements that must be met by the software engineering products, and/or requirements that must be true of the software's performance over time in order to provide a degree of confidence in the software that is commensurate with the software's integrity level.

This International Standard does not prescribe the way in which integrity level determination is integrated with the overall system engineering life cycle processes.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 2382-1:1993, *Information technology - Vocabulary - Part 1: Fundamental terms*.

ISO/IEC 2382-20:1995, *Information technology - Vocabulary - Part 20: System development*.

ISO 8402:1994, *Quality management and quality assurance - Vocabulary*.

IEC 50-191:1990, *International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service*.

IEC 300-3-9:1995, *Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems*.

ISO/IEC 12207:1995, *Information technology - Software life-cycle processes*.

3 Definitions

For the purposes of this International Standard, the definitions given in ISO/IEC 2382-1, ISO/IEC 2382-20, ISO 8402 and IEC 50-191 apply, except as modified or supplemented by the following definitions.

3.1 component: An entity with discrete structure, such as an assembly or software module, within a system considered at a particular level of analysis.

3.2 degree of confidence: In this standard the term degree of confidence is used only to mean the degree of confidence that software conforms to its requirements.

3.3 design authority: The person or organization that is responsible for producing the design of the system.

3.4 failure: The termination of the ability of an item to perform a required function or its inability to perform within previously specified limits.

3.5 fault isolation: The ability of a subsystem to prevent a fault within the subsystem from causing consequential faults in other subsystems.

3.6 function: An aspect of the intended behavior of the system.

3.7 initiating event: An event that can lead to a threat.

3.8 integrity assurance authority: The independent person or organization responsible for assessment of compliance with the integrity requirements.

3.9 integrity level: A denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.

3.10 item: An entity such as a part, component, subsystem, equipment or system that can be individually considered. An item may consist of hardware, software or both.

3.11 mitigating function: A mitigating function is a function that, if provided successfully, will prevent an initiating event from becoming a specified threat.

3.12 risk: A function of the probability of occurrence of a given threat and the potential adverse consequences of that threat's occurrence.

3.13 risk dimension: A perspective from which risk assessment is being made for the system (eg safety, economic, security).

3.14 safety: The expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered.

3.15 security: The protection of system items from accidental or malicious access, use, modification, destruction, or disclosure.

3.16 software integrity level: The integrity level of a software item.