

ICS 35.080
L 77



中华人民共和国国家标准

GB/T 18492—2001
idt ISO/IEC 15026:1998

信息技术 系统及软件完整性级别

Information technology—System and software integrity levels

2001-11-02 发布

2002-06-01 实施

中华人民共和国
国家质量监督检验检疫总局 发布

目 次

前言	Ⅲ
ISO/IEC 前言	Ⅳ
1 范围	1
2 引用标准	1
3 定义	1
4 符号和缩略语	3
5 软件完整性级别框架	3
5.1 如何使用本标准	3
5.2 概貌	3
6 系统完整性级别的确定	5
6.1 风险分析	5
6.2 风险评估	6
6.3 系统完整性级别的确定	6
7 软件完整性级别的确定	6
7.1 软件完整性级别确定前提	7
7.2 软件完整性级别的降低	7
7.3 降低因其失效可能导致一个威胁的软件完整性级别	7
7.4 降低因其失效可能导致不能提供缓减功能的软件完整性级别	8
8 软件完整性需求确定	8
8.1 置信度	8
8.2 在软件中获得置信度的方法	8
8.3 软件置信度与完整性级别的联系	8

前 言

本标准等同采用国际标准 ISO/IEC 15026:1998《信息技术 系统及软件完整性级别》。

本标准定义了与完整性级别相关的概念,定义了确定完整性级别和软件完整性需求的过程,并对每个过程的需求。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准由中国电子技术标准化研究所负责起草。

本标准主要起草人:胡九川、罗锋盈、蔡愉祖。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 15026 由 ISO/IEC JTC1 信息技术联合技术委员会 SC7 软件工程分技术委员会制定。

中华人民共和国国家标准

信息技术 系统及软件完整性级别

GB/T 18492—2001
idt ISO/IEC 15026:1998

Information technology—System and software integrity levels

1 范围

本标准介绍了软件完整性级别的概念和软件完整性需求,定义了与完整性级别相关的概念,定义了确定完整性级别和软件完整性需求的过程,并提出对每个过程的需求。本标准不规定专门的一组完整性级别或软件完整性需求。它们必须依据某一项目的基础在该项目中加以确定。本标准仅适用于软件。系统完整性级别和非软件部件的完整性级别仅在本标准中被用来确定软件部件的完整性级别。

本标准可供软件产品或包含软件产品的系统的开发者、使用者、采购者和评估人员使用,向他们提供关于这些产品和系统和管理上和技术上的支持。

软件完整性级别表示软件特性的取值范围,该范围对将系统风险保持在可容忍的限度内是必需的。对于执行缓减功能的软件而言,此特性是指软件必须执行缓减功能的可靠性。对于因其失效而导致一个系统威胁的软件而言,此特性是指对该失效的频率或概率的限制。

软件完整性需求是软件开发中软件工程过程所必需满足的需求,是软件工程产品所必需满足的需求;或是为提供与软件完整性级别相适应的软件置信度而对软件在某一时段的性能的需求。

本标准未规定将确定软件完整性级别(的工作)同整个系统工程生存期过程结合在一起的方法。

2 引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订。使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语(eqv ISO/IEC 2382-1:1993)

GB/T 5271.20—1994 信息技术词汇 20部分 系统开发(idt ISO/IEC 2382-20:1990)

GB/T 6583—1994 质量管理和质量保证 术语(idt ISO 8402:1994)

GB/T 8566—2001 信息技术 软件生存周期过程(idt ISO/IEC 12207:1995)

IEC 50-191:1990 国际电工词汇,191章:可信性和服务质量

IEC 300-3-9:1995 可信性管理 第3部分:应用指南 第9章:技术系统的风险分析

3 定义

除下述定义所作的修改或补充外,GB/T 5271.1、GB/T 5271.20、GB/T 6583 和 IEC 50-191 中给出的定义适用于本标准。

3.1 部件 component

在一个特定的分析层次上考虑的系统带有分立结构的实体。诸如一个组合或软件模块。

3.2 置信度 degree of confidence

在本标准中,置信度仅用于表示软件同其需求相符合的置信度。

3.3 设计机构 design authority