ICS 35.080
L 77

中华人民共和国国家标准

GB/T 30998—2014

信息技术　软件安全保障规范

Information technology—Software safety assurance specification

2014-09-03 发布　　2015-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出归口。

本标准起草单位:中国电子技术标准化研究院、复旦大学、总装备部武器装备论证研究中心、北京东方通科技股份有限公司、上海计算机软件技术开发中心、万达信息股份有限公司、装备学院。

本标准的主要起草人:王卫国、李海波、丛培勇、冯惠、陈志峰、杨丽蕴、李春青、张鲁峰、钱乐秋、李光亚、龚波。

信息技术　软件安全保障规范

1　范围

本标准规定了获取或开发安全关键软件所必需的软件安全活动、数据和文档。

本标准适用于定制、重用和现货的安全关键软件的开发和获取过程，也适用于固件。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 11457　信息技术　软件工程术语

3　术语、定义和缩略语

3.1　术语和定义

GB/T 11457 中界定的以及下列术语和定义适用于本文件。

3.1.1

事故　accident

造成人员伤亡，职业疾病，设备、财产损坏或损失，环境破坏等的一个或一系列非预期事件。

3.1.2

组件　component

一个系统或子系统的组成元素。

3.1.3

客户　customer

获取其他组织所开发的软件的实体，包括工程、项目、设施。

3.1.4

分解　decomposition

将一个系统或组件划分为组成部分的过程。

3.1.5

失效模式与影响的分析　failure modes and effects analysis

一种自底向上系统的、归纳的、有条理的分析，用于在指定的级别上标识并记录所有可识别的失效模式并详述失效模式的后果。

3.1.6

故障树分析　fault tree analysis

一种故障分析技术，用来识别非期望的系统状态，在系统环境和运行的上下文中对其进行分析以找到所有非期望事件可能出现的可信途经。

3.1.7

故障检测　fault detection

发现故障的能力，判断故障已经发生的过程。