ICS 03.120.01
L 05

中华人民共和国国家标准

GB/T 37407—2019

应用指南　系统可信性工程

Application guide—Engineering of system dependability

(IEC 60300-3-15:2009,Dependability management—
Part 3-15:Application guide—Engineering of system dependability,MOD)

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
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。

本标准使用重新起草法修改采用 IEC 60300-3-15:2009《可信性管理　第 3-15 部分:应用指南　系统可信性工程》。

本标准与 IEC 60300-3-15:2009 相比存在结构变化,新增了附录 A 用于说明技术性差异及其原因,原附录 A～附录 D 分别对应本标准的附录 B～附录 E。

本标准与 IEC 60300-3-15:2009 相比存在技术性差异,这些差异涉及的条款已通过在其外侧页边空白位置的垂直单线(|)进行了标示,附录 A 中给出了相应技术性差异及其原因的一览表。

本标准做了下列编辑性修改:

——将标准名称修改为《应用指南　系统可信性工程》。

——在附录 E 中补充了关于列项的引导语。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国电工电子产品可靠性与维修性标准化技术委员会(SAC/TC 24)归口。

本标准起草单位:工业和信息化部电子第五研究所。

本标准主要起草人:张帆、熊婧。

引　言

当前应用环境中系统变得越来越复杂，系统可信性已经成为一个重要属性，它影响到系统采购的商业策略和系统维修和运营的成本效益。总体而言，系统可信性是系统组件、应用环境、人-机界面、保障服务部署和其他影响因素之间复杂综合作用的结果。

本标准提供了整个系统实现可信性目标的工程指南。对关注的系统，本标准提供的工程方法描述了如何应用相关的科学知识和技术学科以实现需要的系统可信性。

系统可信性在工程上主要体现在四个方面：

——过程；

——实现；

——评估；

——量度。

这些工程学科中的技术过程分布在系统寿命周期的各阶段。本标准描述的技术过程由一系列相关的过程活动支持，这些过程活动确保实现系统每个寿命周期阶段的目标。

本标准适用于通用的有交互功能的系统，交互功能由硬件、软件和人的因素组成，以实现系统的性能目标。在多数情况下，一个功能可以由现有的商业产品实现。一个系统可以连接到其他系统共同形成一个网络。通过定义实体中的应用可以明确区分产品和系统，系统和网络的边界。例如，数字计时器作为一种产品可以同步计算机的操作，计算机作为一个系统可以与办公室的其他计算机连接成一个局域网。应用环境适用于所有类型的系统。用于系统的例子有发电控制系统、容错计算机系统和提供维修保障服务的系统。

可信性工程指南用于通用系统。它不针对有特定应用的系统。出于经济原因和实际应用的需要，大部分系统在整个寿命周期中是可维修的。不可修复系统，如通信卫星、遥感/监测设备和一次性的设备被认为是特殊的系统。他们需要进一步确定具体的应用环境，操作条件和独特的性能特征，以实现任务成功的目标。不可修复的分系统和组件在此不予考虑。通过项目裁剪和可信性管理程序可为指定系统选择一个实现工程可信性的适用流程。

本标准是系统可信性方面标准架构的一部分，以支持可信性管理的 IEC 60300-1 标准。引用文件可用于系统的项目管理活动。它们包括系统相关的可信性元素和任务的识别以及可信性管理评审和可信性项目裁剪的指引。

应用指南　系统可信性工程

1　范围

本标准提供系统可信性的工程指南，并描述贯穿系统寿命周期的系统可信性实现过程。

本标准适用于新系统开发和现有系统改进，涉及硬件、软件和人的因素组成的系统功能的交互；也适用于为寻求系统信息和系统集成准则的分系统和产品的供应商。本标准为可信性目标的实现结果提供了系统可信性评估和验证的方法和工具。

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 8566　信息技术　软件生存周期过程(GB/T 8566—2007，ISO/IEC 12207：1995，MOD)

GB/T 20438(所有部分)　电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分)]

GB/T 20438.1　电气/电子/可编程电子安全相关系统的功能安全　第1部分：一般要求(GB/T 20438.1—2017，IEC 61508-1：2010，IDT)

GB/T 20917　软件工程　软件测量过程(GB/T 20917—2007，ISO/IEC 15939：2002，IDT)

GB/T 22032　系统工程　系统生存周期过程(GB/T 22032—2008，ISO/IEC 15288：2002，IDT)

IEC 60300-1　可信性管理　第1部分：管理和应用指南(Dependability management—Part 1：Guidance for management and application)

IEC 60300-3-1　可信性管理　第3-1部分：应用指南　可信性分析技术　方法学指南(Dependability management—Part 3-1：Application guide—Analysis techniques for dependability—Guide on methodology)

IEC 60300-3-9　可信性管理　第3-9部分：应用指南　技术系统的风险分析(Dependability management—Part 3：Application guide—Section 9：Risk analysis of technological systems)

IEC 62347　系统可信性规范指南(Guidance on system dependability specifications)

3　术语和定义

下列术语和定义适用于本文件。

3.1

系统　system

共同满足特定要求的相互关联产品的集合。

注1：系统通常从实施一个确切功能的角度进行定义。

注2：假设系统由一个假想的边界构成，系统与环境和其他外部系统连接相交之处即是该边界。

注3：系统可能需要外部(即系统边界之外)资源来操作。

注4：系统结构可能是分层的，例如：系统、子系统和部件等。