ICS 03.100.40;03.120.01;21.020
CCS L 05

中华人民共和国国家标准

GB/T 48410—2026/IEC 62853:2018

开放系统可信性

Open systems dependability

（IEC 62853 :2018,IDT）

2026-10-30 发布　　2027-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　开放系统可信性 …… 4
4.1　开放系统 …… 4
4.2　开放系统特有的可信性问题 …… 5
4.3　目标 …… 5
4.4　实现开放系统的可信性 …… 5
4.5　恢复力和容错的关系 …… 6
5　符合性 …… 6
6　实现开放系统可信性的过程视图 …… 6
6.1　概述 …… 6
6.2　共识构建过程视图 …… 7
6.3　责任追溯过程视图 …… 11
6.4　失效响应过程视图 …… 18
6.5　变更适应过程视图 …… 24
附录A（资料性）　开放系统可信性的生命周期模型示例 …… 32
A.1　概述 …… 32
A.2　开放系统可信性工程(DEOS)生命周期模型 …… 32
A.3　保修链管理(WCM)生命周期模型 …… 34
附录B（资料性）　可信性实证数据包的示例模板 …… 36
B.1　概述 …… 36
B.2　共识构建论证 …… 36
B.3　责任追溯论证 …… 38
B.4　失效响应论证 …… 40
B.5　变更适应论证 …… 44
附录C（资料性）　智能电网示例 …… 47
C.1　概述 …… 47
C.2　背景 …… 47
C.3　智能电网可信性实证数据包的构建 …… 47
C.4　变更适应循环 …… 50
C.5　失效响应循环 …… 51
参考文献 …… 52

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件等同采用IEC 62853:2018《开放系统可信性》。

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专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件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。

本文件起草单位:工业和信息化部电子第五研究所、中国航天电子技术研究院、中国航天标准化研究所、北京电子工程总体研究所。

本文件主要起草人:胡宁、陈冰泉、张晨光、高馨、雷庭、王晋婧、于敏、潘勇、杨洪旗、高滢、李应选、李庚雨、原艳斌、李泉洲、李然。

引　言

开放系统是一种边界、功能和结构随时间变化的系统，对其认知和描述因视角不同而不同。由于开放系统在整个生命周期中不断变化，自身存在不确定性，系统在运行过程中易受到多种因素的影响导致服务中断或终止，造成损失。因此，保证系统在发生失效和变化时，也能长期保持服务连续性，维持系统正常运行至关重要。而开放系统可信性是指该系统能够适应目标、目的、环境和实际性能的变化，并持续保持对利益相关方的责任，确保能在需要时按要求提供预期服务的能力。因此，实现开放系统可信性，提高开放系统可信性水平，有助于保证系统安全、稳定运行，维持服务连续性。

本文件通过给出变更适应、责任追溯、失效响应、共识构建四个过程视图的活动、过程和输出等内容为实现开放系统可信性提供指导，选择并组合了 GB/T 22032—2021 中系统生命周期过程、活动和任务，在 IEC 60300-1 的基础上提供了开放系统可信性管理的指导原则。

本文件预期的读者包括用户、负责保证开放系统可信性需求得到满足的所有者、客户、组织。组织涵盖各种类型和规模的企业，政府部门、企事业单位和非营利协会等公共和私有机构。

开放系统可信性

1 范围

本文件提供了一套实现开放系统生命周期可信性的需求的相关指南。

本文件基于 IEC 60300-1,提供了适应开放系统特性所需的变更细节。基于 GB/T 22032—2021 定义了一组识别系统生命周期过程集合的过程视图。

本文件适用于包括硬件、软件和人因方面,或这些方面的任意组合的产品、系统、过程或服务的生命周期。

开放系统特别容易遭受攻击,因此需重视其信息安全。

本文件能用于提高开放系统的可信性,并确保开放系统特定的过程视图实现其预期结果。有助于组织定义开放系统实现可信性目标所需的活动和任务,包括系统生命周期中与可信性相关的沟通、可信性评估和可信性评价。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 22032—2021 系统与软件工程 系统生存周期过程(ISO/IEC/IEEE 15288:2015,IDT)

IEC 60050-192 电工术语 第 192 部分:可信性 (International electrotechnical vocabulary—Part 192:Dependability)

注:GB/T 2900.99—2016 电工术语 可信性(IEC60050-192:2015,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)

注:GB/T 36615—2018 可信性管理 管理和应用指南(IEC 60300-1:2014,IDT)

3 术语和定义

IEC 60050-192 界定的以及下列术语和定义适用于本文件。

3.1

担责 accountability

组织能为其决策和活动接受其治理机构、监管机构乃至利益相关方问责的状态。

注 1:担责通常包括社会责任。

注 2:GB/T 36000—2015 中描述担责包括组织对控制利益方就管理负责的义务,及对法律机构就法律法规负责的义务。组织就其决策和活动对社会与环境的总体影响负责,也通常意味着该组织对受其决策和活动影响的对象负责,根据影响的性质和情况而定。

注 3:GB/T 2612.1—2010 中定义了个人、组织和团体对其行为负责的准则,并可能被要求向他人解释。

[来源:GB/T 36000—2015,2.1,有修改]