ICS 33.050
CCS M 30

团　体　标　准

T/TAF 331.1—2026

信息通信产品运行安全完整性 第1部分：总体要求

Operation Safety integrity of information and communication product—Part 1: General requirements

2026-02-09 发布　　2026-02-09 实施

电信终端产业协会　发布

版权声明

邮箱：tafrb@taf.org.cn

电话：010-8205280

目　　次

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。

本文件是 T/TAF 331《信息通信产品运行安全完整性》的第 1 部分。T/TAF 331 已经发布了以下部分：

——第 1 部分：总体要求。

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。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、中兴通讯股份有限公司、成都泰瑞通信设备检测有限公司、武汉网锐检测科技有限公司、上海泰峰检测认证有限公司、烽火通信科技股份有限公司、西安通和电信设备检测有限公司、博鼎实华（北京）技术有限公司。

本文件主要起草人：路晔绵、张治兵、吴荣春、陈鹏、钟依彤、周继华、吴翔宇、陈玺、龚志红、宋祥烈、李丹、邓科、王羲文、高露凯、刘向东、王玥。

引　言

T/TAF 331旨在建立适用于信息通信产品的运行安全完整性体系，明确信息通信产品运行安全完整性要求和评估方法，通过规范指导，降低信息通信产品故障和失效概率，提高信息通信产品安全性，从而降低因信息通信产品故障和失效导致的网络运行事故发生概率。T/TAF 331拟由3个部分构成。

——第1部分：总体要求。目的在于明确信息通信产品运行安全完整性总体要求，包含信息通信产品运行安全完整性概述以及系统、硬件、软件运行安全完整性要求。

——第2部分：等级确定指南。目的在于明确信息通信产品运行安全完整性等级确定的基本方法。

——第3部分：评估指南。目的在于明确信息通信产品运行安全完整性评估流程及具体方法。

信息通信产品运行安全完整性　第1部分：总体要求

1　范围

本文件规定了信息通信产品运行安全完整性总体要求，包含信息通信产品运行安全完整性概述、生命周期要求以及各阶段系统、硬件、软件运行安全完整性要求。

本文件适用于信息通信产品运行安全完整性设计、实现、评估等环节。

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 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

3　术语和定义

GB/T 20438界定的以及下列术语和定义适用于本文件。

3.1

安全完整性　safety integrity

在规定的时间内和规定的条件下，信息通信产品成功执行规定的安全功能的概率。

[来源：GB/T 20438.4—2017，3.5.4，有修改]

3.2

安全状态　safe state

在故障（3.4）或失效（3.8）情况下，没有不合理风险（3.3）的运行模式。

3.3

风险　risk

网络运行事故发生的可能性及其严重性的组合。

3.4

故障　fault

可能导致功能单元执行要求功能的能力减低或丧失的异常状况。

[来源：GB/T 20438.4—2017，3.6.1]

3.5

故障容错时间间隔　fault tolerant time interval

安全功能未被激活情况下，从故障（3.4）或失效（3.8）发生到可能发生网络运行事故的最短时间间隔。

3.6

降级　degradation

功能缩减、性能降低或两者均有的状态。

3.7

鲁棒性 robustness

在无效输入或有压力的环境条件下正确工作的能力。

3.8

失效 failure

可能导致预期行为终止的情况。

3.9

失效率 failure rate

工作到某一时刻尚未失效的实体，在该时刻后，单位时间内发生失效的概率。

3.10

危险 hazard

导致网络运行事故的潜在根源。

3.11

信息通信产品 information and communication product

组成信息通信网络或提供信息通信服务的软硬件或系统。

3.12

运行安全完整性 operation safety integrity

信息通信产品成功执行避免或降低网络运行风险（3.3）的安全功能的概率。

3.13

诊断 diagnostic

对故障（3.4）的探测。

3.14

诊断覆盖率 diagnostic coverage

由实现的安全功能探测或控制的失效率（3.9）占总体失效率（3.9）的百分比。

3.15

组件 element

由一个或多个软硬件单元组成的执行一个或多个安全功能的实体。

4 缩略语

下列缩略语适用于本文件。

OSIL：运行安全完整性等级（Operation Safety Integrity Level）

5 概述

信息通信产品发生故障和失效是导致网络运行事故的重要原因之一，为保证网络运行安全稳定，有必要降低信息通信产品故障和失效发生概率，或减轻因信息通信产品故障和失效导致的网络运行事故的发生可能性及严重性。本文将信息通信产品降低故障与失效风险的能力定义为运行安全完整性。

信息通信产品运行安全完整性等级定义为OSIL。本文参考GB/T 20438，将OSIL分为4个等级，即OSIL 1~OSIL 4，其中OSIL 4为最高级。OSIL等级越高，意味着信息通信产品发生故障和失效的概率越低，或因信息通信产品故障和失效导致网络运行事故的可能性越低。

为保证信息通信产品运行安全，达到相应OSIL等级的安全要求，应在信息通信产品安全生命周期的各阶段开展合适的活动，采取适当的技术和措施，以提高信息通信产品的安全性。本部分第6章介绍了

信息通信产品安全生命周期要求，其中每个阶段的详细要求在第7～14章中进行描述。附录A给出了为满足对应的OSIL等级要求，在信息通信产品安全生命周期各个阶段选择技术和措施的指南。

6 安全生命周期

为保证信息通信产品运行安全，其安全生命周期设计宜包含图1中所示的典型安全生命周期阶段，表1给出了图1中各阶段的概述。图1所示的安全生命周期阶段可进行裁剪，但需提供合理的裁剪理由，并经评估确认所进行的裁剪不会对信息通信产品安全性造成影响。

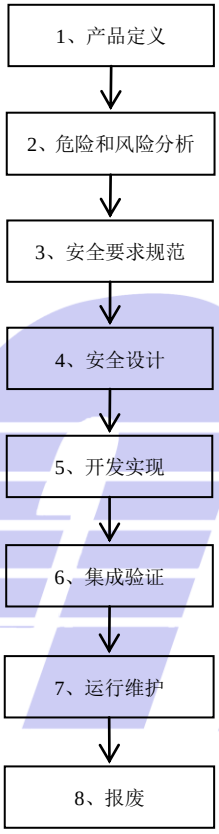

图1 典型安全生命周期阶段

表 1 典型安全生命周期阶段概述

安全生命周期阶段		内容	要求所在章节	输出
图1中的编号	标题			
1	产品定义	确定产品应用场景、功能、组成部分、边界，以及与环境的依赖性和交互等	7	产品描述
2	危险和风险分析	确定产品可能的故障和失效模式，分析可能造成的危险和危险事件，确定产品运行安全目标及其对应的运行安全完整性等级OSIL	8	产品运行安全目标和对应的运行安全完整性等级OSIL

表 2　典型安全生命周期阶段概述（续）

安全生命周期阶段		内容	要求所在章节	输出
图1中的编号	标题			
3	安全要求规范	根据产品运行安全目标和对应的OSIL等级，明确产品安全功能要求及安全完整性要求	9	产品安全要求规范
4	安全设计	根据安全要求规范，确定安全功能实现方案	10	产品安全设计规范
5	开发实现	根据产品安全设计规范，完成产品安全功能的开发和实现，使其满足安全功能和对应的OSIL等级要求	11	满足产品安全要求规范和安全设计规范的产品
6	集成验证	将产品各部分进行集成；根据要求的安全功能及对应的OSIL等级，对产品安全功能进行适当的安全测试验证，确认产品满足安全要求	12	产品安全测试验证规范；产品安全测试验证结果
7	运行维护	明确产品运行维护期间的安全要求	13	产品运行维护指导说明
8	报废	明确产品报废的安全要求	14	产品报废指导说明

7　产品定义

7.1　目的

本阶段的目的是：

a)　对产品进行描述，确定产品应用场景、功能、组成部分、边界，以及与环境的依赖性和交互；

b)　为充分理解产品提供支持,以便执行后续阶段的活动。

7.2　内容要求

产品定义阶段要求如下：

a)　应给出产品应用场景；

b)　应给出产品的功能，包括其运行模式或运行状态；

c)　应给出产品的组成部分和边界，以明确危险和风险分析的范围；

d)　应给出产品与运行环境的交互接口；

e)　应给出产品的约束，例如功能依赖性、与运行环境的依赖性；

f)　如适用，应给出产品质量、性能、功能可用性的要求；

g)　应给出与产品有关的假设、约束、限制条件等。

7.3　输出成果要求

此阶段执行完成后，应形成产品描述文档，其中内容应满足7.2小节的要求。

8　危险和风险分析

8.1 目的

本阶段的目的是：

a) 识别由产品功能异常表现引发的潜在危险；

b) 确定防止危险事件发生或减轻其危害程度的运行安全目标及相应的OSIL等级，以避免不合理的风险。

8.2 内容要求

危险和风险分析阶段要求如下：

a) 应针对产品系统架构设计、硬件、软件、接口交互等各个环节，逐一识别故障和失效模式；

b) 应考虑产品在正常运行、峰值负载、软件升级等各类运行模式下的潜在风险；

c) 应针对每个故障和失效分析其发生危险事件的可能性和后果，确定其运行安全完整性等级OSIL；

d) 应为每个OSIL等级大于等于1的危险事件确定一个运行安全目标；若确定的运行安全目标是类似的，可将其合并为一个运行安全目标；

e) 为危险事件所确定的OSIL等级应分配给对应的运行安全目标；若将类似的运行安全目标合并为一个运行安全目标，应将最高的OSIL等级分配给合并后的运行安全目标；

f) 在确定OSIL等级时，应识别其中使用到的或从中得出的假设（例如，存在其他风险降低措施的假设）；

g) 在危险和风险分析过程中，不应考虑将要实施或已经实施的安全机制，确保风险分析反映真实原始风险水平。

8.3 输出成果要求

在危险和风险分析阶段执行完成后，应输出以下成果：

a) 危险和风险分析报告，其中内容应满足8.2小节的要求；

b) 产品运行安全目标和对应的运行安全完整性等级OSIL列表，明确每个运行安全目标（或合并目标）的具体内容、适用场景，及其对应的OSIL等级，为后续安全设计提供直接依据。

9 安全要求规范

9.1 目的

本阶段的目的是：

根据危险和风险分析阶段得出的运行安全目标，明确产品应实现的安全功能和对应的OSIL等级。

9.2 内容要求

安全要求规范阶段要求如下：

a) 安全功能要求应由运行安全目标导出，并考虑系统架构设计情况；

b) 应为每一个运行安全目标导出至少一项安全功能要求；但若运行安全目标的实现依赖于外部措施，应导出由外部措施实施的安全要求，并在适用时规定与外部措施接口的安全功能要求；

c) 应将运行安全目标对应的OSIL等级分配给对应的安全功能要求，当一个安全功能要求由多个运行安全目标导出时，应将多个运行安全目标中最高的OSIL等级分配给该安全功能要求；

d) 如果适用，确定安全功能要求时应考虑以下内容：

1) 系统自身故障的诊断、告警和控制；

2） 与当前产品有相互影响的外部组件中故障的诊断、告警和控制；
3） 使系统实现或维持在安全状态的安全功能；
4） 定义和执行告警和降级策略的安全功能；
5） 故障容错时间间隔。

e） 在确定硬件安全功能要求时，如果适用，还应考虑以下内容：
1） 为控制内部失效的硬件安全功能；
2） 为控制或容忍外部失效的硬件安全功能；
3） 为符合其他组件安全需求的硬件安全功能；
4） 为探测内外部失效的硬件安全功能；
5） 硬件性能要求。

f） 在确定软件安全功能要求时，如果适用，还应考虑以下内容：
1） 软件自监控；
2） 对交互硬件运行状态的监控；
3） 安全功能在线（即在预期的运行环境中运行时）自检测试的相关功能；
4） 安全配置数据的检测和访问控制；
5） 应对错误输入的鲁棒性；
6） 不同功能之间的独立性或免于干扰；
7） 容量和响应时间性能。

g） 如果可以通过过渡到或保持一个或多个安全状态来避免运行安全目标的违背，那么应定义相应的安全状态；

h） 应保持安全功能要求与运行安全目标的一致性和符合性，应提供证据证明从安全功能要求到运行安全目标的可追溯性。

9.3 输出成果要求

此阶段执行完成后，应输出产品安全要求规范，明确产品安全功能要求及对应的OSIL等级，同时安全要求规范内容应满足9.2小节的要求。

10 安全设计

10.1 目的

本阶段的目的是：
根据产品安全要求规范，确定安全功能实现方案，确定各层级架构设计。

10.2 内容要求

10.2.1 通用要求

安全设计阶段通用要求如下：

a） 各层级架构设计应实现安全要求规范中的安全功能要求；

b） 应明确在产品安全生命周期各阶段中为达到所需OSIL等级所必需的技术和措施；

c） 应在安全设计过程中考虑开发实现、运行维护和报废环节的安全需求，如运行时监控；

d） 为了避免系统性故障,各层级架构设计都应具有以下特征：
1） 模块化；
2） 适当的颗粒度；

3） 清晰准确；
4） 可验证性；
5） 可维护性。

e） 安全设计过程中新识别的尚未被当前安全功能涵盖的危险和风险，应回退到合适的生命周期阶段进行更新；

f） 应保持安全架构与安全要求规范的一致性和符合性，应提供证据证明从安全架构到安全要求规范的可追溯性。

10.2.2 系统层面要求

系统层面安全设计附加要求如下：

a） 系统架构设计应考虑以下内容：
1） 与实现运行安全相关的预期的软硬件组件技术能力；
2） 系统内部和外部接口，特别是软硬件接口；
3） 在系统集成过程中执行测试的能力。

b） 软硬件接口设计应包括以下内容：
1） 由软件控制的硬件元器件以及支持软件运行的硬件资源；
2） 硬件设备的相关运行模式和相关配置参数；
3） 支持软件分区隔离的硬件特征；
4） 软件对硬件设备的访问机制；
5） 需要在软件中实现的对硬件的诊断特性。

10.2.3 硬件层面要求

硬件层面安全设计附加要求如下：

a） 硬件架构设计应实现安全要求规范中的硬件安全要求；

b） 应明确硬件系统边界接口，并细化系统架构设计中软硬件接口设计中对硬件的要求；

c） 应保证硬件安全设计及细化的软硬件接口设计与系统安全设计的符合性；

d） 每个硬件组件都应按照分配给它的所有安全要求中最高的OSIL等级来开发实现；

e） 应考虑硬件元器件或硬件组件的运行条件，以确保硬件元器件或硬件组件在其规格范围内运行，以避免其由于预期使用而发生失效；

f） 在硬件架构设计时，应考虑硬件组件失效的非功能性原因，如果适用，可包括以下的影响因素：温度、振动、水、灰尘、电磁干扰、噪声因素或来自硬件架构的其他硬件组件或其所在环境的串扰。

10.2.4 软件层面

软件层面安全设计附加要求如下：

a） 软件架构设计应实现安全要求规范中的软件安全要求；

b） 进行软件架构设计时应考虑以下内容：
1） 已定义的系统和硬件的配置；
2） 已明确的软硬件接口设计；
3） 硬件架构设计中对软件的安全要求；
4） 对软件有影响的产品、系统或者硬件的每个运行模式以及运行模式之间的转换；
5） 集成测试中软件架构的可测试性。

c） 适用时，软件架构设计应考虑以下内容：

1） 软件结构的分级层次；
2） 软件组件的分区隔离；
3） 控制流和执行时序；
4） 数据类型和它们的特征参数；
5） 数据处理的逻辑顺序；
6） 外部接口；
7） 全局变量；
8） 通过接口和全局变量传递的数据流；
9） 所需运行时间、存储空间、通信资源等的限制；
10） 架构的范围和外部依赖的约束；
11） 错误探测和错误处理安全机制；
12） 冗余设计。

d） 软硬件接口设计应细化到可以通过软件正确控制和使用硬件的程度，并应描述硬件和软件间与安全相关的每个依赖性；

e） 应保证软件安全设计及细化的软硬件接口设计与系统安全设计的符合性。

10.3 输出成果要求

此阶段执行完成后，应输出产品安全设计规范，内容应满足10.2小节的要求。

11 开发实现

11.1 目的

本阶段的目的是：

根据产品安全设计规范，完成产品安全功能的开发和实现，使其满足安全功能和对应的OSIL等级要求。

11.2 内容要求

11.2.1 通用要求

开发实现阶段通用要求如下：

a） 应按照产品设计规范，选择符合OSIL等级要求的技术和措施完成产品开发和实现；

b） 在开发实现过程中，应整理安全手册，明确系统配置、运行环境、运行、维护、故障检测等内容。

11.2.2 系统层面要求

系统层面开发实现阶段附加要求如下：

a） 初步开发完成后，应在系统层面进行分析，确定是否有任何之前未曾发现的合理可预见的故障或失效可能导致危险的情况；

b） 开发实现过程中新识别的尚未被当前安全功能涵盖的危险和风险，应回退到合适的生命周期阶段进行更新。

11.2.3 硬件层面要求

硬件层面开发实现阶段附加要求如下：

a) 每个硬件组件应按照分配给它的任何需求的最高的OSIL等级来进行开发实现；
b) 为了满足硬件层面的运行安全完整性要求，不同OSIL等级下硬件失效率和诊断覆盖率的应满足表2要求；
c) 硬件失效率可通过以下途径获取：
   1) 基于国家标准或行业标准采集的数据；
   2) 基于在役组件在类似应用和环境下的现场反馈；
   3) 基于特定测试的结果。
d) 应给出诊断覆盖率的推导证明材料；
e) 如果适用，应满足国家标准或行业标准中对于硬件性能的各项要求。

表 3 不同 OSIL 等级下硬件失效率和诊断覆盖率要求

硬件失效率	诊断覆盖率		
	高（≥99%）	中（≥90%）	低（≥60%）
≤10^{-7}	OSIL 4	OSIL 3	OSIL 2
≤10^{-6}	OSIL 3	OSIL 2	OSIL 1
≤10^{-5}	OSIL 2	OSIL 1	--

11.2.4 软件层面要求

软件层面开发实现阶段附加要求如下：
a) 每个软件组件应按照分配给它的任何需求的最高的OSIL等级来进行开发实现；
b) 如果使用软件分区隔离实现软件组件间免于干扰，那么应确保：
   1) 一个软件分区内的任务彼此之间不能干扰；
   2) 一个软件分区不能改变其他软件分区的代码或数据,也不能控制其他软件分区的非共享资源；
   3) 一个软件分区从共享资源获取的服务不能被另一个软件分区影响，包括相关资源的性能，以及对资源调度访问的使用率、延迟、抖动和持续时间等。
c) 当软件组件的安全性受配置数据影响时，应使用适当的技术和措施以防止在配置数据的生成、装载和修改期间引入故障，并确保配置数据正确地描述应用逻辑；
d) 应选择合适的编程语言和开发编程工具实现软件组件的开发，应对开发编程工具进行安全评估和配置管理；
e) 代码开发应遵循安全编程规范，避免使用不安全的函数；
f) 应规定良好的编程习惯，以保证代码可读、可理解、可测试和可验证；
g) 开发完成后应进行源代码安全审计，并修补审计中发现的安全缺陷。

11.3 输出成果要求

此阶段执行完成后，应输出满足11.2小节要求的产品和安全手册。

12 集成验证

12.1 目的

本阶段的目的是：

a） 将产品各部分进行集成；
b） 验证安全要求规范中明确的安全要求及安全设计中明确的安全架构是否得到正确实施；
c） 提供证据证明所集成的产品满足安全要求。

12.2 内容要求

12.2.1 通用要求

集成验证阶段通用要求如下：
a） 产品的各个要素应按照安全设计中给出的架构进行集成；
b） 产品各要素在独立开发时未解决的与其他要素相关的问题，应在集成环节得到处理；
c） 应对集成系统的所有变更进行影响分析，影响分析应确定所有受影响的模块，在必要时回退到之前合适的生命周期阶段进行重新操作；
d） 应根据安全设计和开发实现情况制定安全测试验证规范，其中应包含以下内容：
   1） 测试验证用例；
   2） 测试工具、设备、配置描述等；
   3） 判定通过的准则和预期结果。
e） 应根据安全测试验证规范进行测试；
f） 在安全测试验证过程中，应考虑所有的运行场景及配置情况；
g） 在安全测试验证过程中，应验证设计开发期间所作假设的有效性；
h） 应保证在安全测试验证过程中全面覆盖安全要求规范中所有安全要求的验证，并提供覆盖率证据；
i） 安全测试验证的结果应归档，记录实际测试结果以及是否满足预期结果；若存在失败的安全测试，应记录失败的原因以及相应的修正措施；若修正失败时对系统进行了变更，应进行影响分析，必要时进行生命周期阶段的回退。

12.2.2 系统层面要求

系统层面应针对以下内容进行安全测试验证：
a） 安全要求规范中所有安全功能的正确执行；
b） 跨软硬件模块的协同功能；
c） 安全功能的性能、准确性和时序；
d） 内外部接口的一致性和正确性；
e） 鲁棒性（如高并发请求、长时间运行场景下的测试）。

12.2.3 硬件层面要求

硬件层面安全测试验证的要求如下：
a） 硬件安全测试验证应与系统安全测试验证规定的策略相协调；
b） 应针对以下内容进行安全测试验证：
   1） 应验证硬件安全要求实现的完整性和正确性；
   2） 应验证硬件组件内外部接口的一致性和正确性；
   3） 应对硬件性能进行测试，以保证其满足需求；
   4） 应验证硬件在环境和运行应力因素下的耐用性和鲁棒性。

12.2.4 软件层面要求

软件层面安全测试验证的要求如下：

a) 软件安全测试验证应与系统安全测试验证规定的策略相协调；

b) 应针对以下内容进行安全测试验证：

1) 应验证软件安全要求实现的完整性和正确性；

2) 应验证软件组件内外部接口的一致性和正确性；

3) 应验证对错误输入的鲁棒性。

c) 软件安全测试环境应考虑目标环境要求，若安全测试无法在目标环境或与目标环境配置相当的环境中执行，应分析测试环境和目标环境之间的差异，证明在测试环境下执行的测试对于软件正式运行的有效性。

12.3 输出成果要求

此阶段执行完成后，应输出以下成果：

a) 满足12.2小节要求的安全测试验证规范，包含所有测试验证用例、测试环境描述、判定通过的准则、预期结果等内容；

b) 安全测试验证报告，记录安全测试验证的所有结果，其结果应能证明所集成的产品满足安全要求规范中的安全要求。

13 运行维护

13.1 目的

本阶段的目的是：

制定必要的规程，为运维人员明确产品在运行、维护和变更情形下的安全要求，确保产品在运行维护环节的安全。

13.2 内容要求

运行维护阶段要求如下：

a) 应编制产品运行维护指导说明，应包含以下内容：

1) 产品主要功能及其运行模式的说明；

2) 产品安全配置说明；

3) 正确使用产品的有关指导说明和警告；

4) 维护和维修的要求；

5) 报警和降级策略；

6) 现场监控操作；

7) 产品升级、变更操作说明；

8) 常见故障诊断及处置流程；

9) 运维人员能力要求；

10) 在之前生命周期阶段识别的运行维护安全要求。

b) 若运行维护阶段存在新识别的尚未被当前安全功能涵盖的危险和风险，应回退到合适的生命周期阶段进行更新。

13.3 输出成果要求

此阶段执行完成后，应输出满足13.2小节要求的产品运行维护指导说明。

14 报废

14.1 目的

本阶段的目的是：

制定必要的规程，为运维人员明确产品在报废或处置环节的安全要求，确保在产品报废或处置活动中或活动后，整个产品仍具有适当的安全功能，防范数据泄露、非法控制等风险。

14.2 内容要求

报废阶段要求如下：

a) 应制定报废指导说明，明确产品在报废处置过程中应采用的活动和措施,以确保其安全报废；
b) 在制定报废指导说明时，应考虑在之前生命周期阶段识别的报废环节安全要求；
c) 若该阶段存在新识别的尚未被当前安全功能涵盖的危险和风险，应回退到合适的生命周期阶段进行更新。

14.3 输出成果要求

此阶段执行完成后，应输出满足14.2小节要求的产品报废指导说明。

附 录 A
（规范性）
技术和措施选择指南

A.1 概述

本附录中表格内容的说明如下：

a) 表格中标识为“R”的方法为推荐方法，标识为“HR”的方法为强烈推荐方法；
b) 在表格最左侧列以顺序号标明的项是独立项，独立项只存在适用和不适用的问题；
c) 在表格最左侧列以数字后加字母标明的项是选择项，可从中选择一种或几种技术/措施使用，至少选择一种，优先选择强烈推荐的方法；
d) 允许使用未列入表中的其他方法替代表格中的已有方法，此种情况下，应给出满足相关要求的理由；
e) 在某一OSIL等级下，独立项中标识为“HR”的方法即为本文件要求应在当前OSIL等级下选用的方法，除非存在下述两种情况：
   1) 使用未列入表中的其他方法替代了标识为“HR”的方法，并给出了其满足相关要求的合理理由；
   2) 当前方法不适用，并给出了合理理由。

A.2 在生命周期各阶段系统层面控制故障和失效的技术和措施

A.2.1 系统安全设计阶段的技术和措施

系统安全设计阶段应采取的技术和措施如表A.1所示。

表A.1 系统设计阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	结构化设计	HR	HR	HR	HR
2	模块化	HR	HR	HR	HR
3a	半形式化方法	R	R	HR	HR
3b	检查表	--	R	R	R
3c	形式化方法	--	--	R	HR

A.2.2 系统集成验证阶段的技术和措施

系统集成验证阶段应采取的技术和措施如表A.2所示。

表A.2 系统集成验证阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	黑盒测试	HR	HR	HR	HR
2a	现场经验分析	R	R	R	R
2b	边界值分析	R	R	HR	HR
2c	基于知识或经验的错误猜测法	R	R	HR	HR
2d	功能的相关性分析	R	R	HR	HR

表A.2　系统集成验证阶段的技术和措施（续）

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
2e	环境条件和操作用例分析	R	HR	HR	HR

A.3 在生命周期各阶段硬件层面控制故障和失效的技术和措施

A.3.1　硬件安全设计阶段的技术和措施

硬件安全设计阶段应采取的技术和措施如表A.3所示。

表A.3　硬件设计阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	分层设计	R	R	R	R
2	硬件组件的精确定义接口	HR	HR	HR	HR
3	避免不必要的接口复杂性	R	R	R	R
4	避免不必要的硬件组件复杂性	R	R	R	R
5	可维护性	R	R	HR	HR
6	可测试性	R	R	HR	HR

A.3.2　硬件开发实现阶段的技术和措施

硬件开发实现阶段应采取的技术和措施如表A.4所示。

表A.4　硬件开发实现阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1a	仿真	--	R	R	HR
1b	硬件检查或硬件走查	--	R	R	R

A.3.3　硬件集成验证阶段的技术和措施

硬件集成验证阶段应采取的技术和措施如表A.5所示。

表A.5　硬件集成验证阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	功能测试	HR	HR	HR	HR
2a	现场经验分析	R	R	R	R
2b	边界值分析	R	R	HR	HR
2c	基于知识或经验的错误猜测法	HR	HR	HR	HR
2d	功能的相关性分析	R	R	HR	HR
2e	环境条件和操作用例分析	R	HR	HR	HR
2f	内部和外部接口分析	R	HR	HR	HR
2g	重要变量分析	HR	HR	HR	HR

A.4 在生命周期各阶段软件层面控制故障和失效的技术和措施

A.4.1 软件安全设计阶段的技术和措施

软件安全设计阶段应采取的技术和措施如表A.6所示。

表A.6 软件安全设计阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	故障检测	--	R	HR	HR
2	错误检测代码	R	R	R	HR
3	失效断言编程	R	R	R	HR
4a	故障恢复重试机制	R	R	--	--
4b	适度降级	R	R	HR	HR
5	模块化方法	HR	HR	HR	HR
6a	半形式化方法	R	R	HR	HR
6b	形式化方法	--	R	R	HR

A.4.2 软件开发实现阶段的技术和措施

软件开发实现阶段应采取的技术和措施如表A.7所示。

表A.7 软件开发实现阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	适当的编程语言	HR	HR	HR	HR
2a	已评估的工具和已评估的编译器	R	HR	HR	HR
2b	工具和编译器：通过使用提高置信度	HR	HR	HR	HR
3	模块化方法	HR	HR	HR	HR
4	结构化编程	HR	HR	HR	HR
5	设计和编码标准	R	HR	HR	HR
6	防御性编程	--	R	HR	HR

A.4.3 软件集成验证阶段的技术和措施

软件集成验证阶段应采取的技术和措施如表A.8所示。

表A.8 软件集成验证阶段的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	概率测试	--	R	R	R
2	动态分析和测试	R	HR	HR	HR
3	数据记录和分析	HR	HR	HR	HR
3	功能和黑盒测试	HR	HR	HR	HR
4	性能测试	R	R	HR	HR

表A.8　软件集成验证阶段的技术和措施（续）

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
5	接口测试	R	R	HR	HR
6	测试管理和自动化工具	R	R	HR	HR
7	形式化验证	--	--	R	R

A.4.4　软件变更的技术和措施

软件变更情形下应采取的技术和措施如表A.9所示。

表A.9　软件变更的技术和措施

序号	技术/措施	OSIL 1	OSIL 2	OSIL 3	OSIL 4
1	影响分析	HR	HR	HR	HR
2	变更模块的再验证	HR	HR	HR	HR
3	受影响模块的再验证	R	HR	HR	HR
3	回归确认	R	HR	HR	HR
4	软件配置管理	HR	HR	HR	HR
5	数据记录和分析	HR	HR	HR	HR

电信终端产业协会团体标准

信息通信产品运行安全完整性　第 1 部分：总体要求

T/TAF 331.1—2026

*

电信终端产业协会发布
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版下载网址：www.taf.org.cn