ICS 03.120.10
CCS A 00

团体标准

T/GRTIA 1-2025

城市轨道交通 装备可信性管理体系 要求

Intercity railway—Equipment dependability management system—Requirements

2025 - 6 - 26 发布　　2025 - 7- 5 实施

广州市轨道交通产业联盟　　发 布

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》和GB/T 20001.11—2022《标准编写规则 第11部分 管理体系标准》的规定起草。

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。

本文件由广州市轨道交通产业联盟提出、归口、解释并组织实施。

本文件起草单位：西南交通大学、广州地铁集团有限公司、广州中车轨道交通装备有限公司、交铁检验认证中心（成都）有限公司、中国标准化研究院、广州市轨道交通产业联盟、城市轨道交通系统安全与运维保障国家工程研究中心、佛山市地铁建设有限公司、东莞市轨道交通有限公司、中山市轨道交通有限公司、广州地铁设计院、中车株洲电机有限公司、中车广东轨道交通车辆有限公司、广州大湾区轨道交通产业投资集团、佳都科技集团股份有限公司、广东华之源信息工程有限公司、白云电气集团有限公司、中电科普天科技股份有限公司、广州广电运通智能科技有限公司、广州轨道交通检验检测认证有限公司、广州计量检测技术研究院、中国电子科技集团公司第七研究所、广州鼎汉轨道交通车辆装备有限公司、石家庄国祥运输设备有限公司、广州朗进轨道交通设备有限公司、广州广冷华旭制冷空调实业有限公司、广州精益运输制冷设备有限公司、深圳恒之源技术股份有限公司、深圳市垅运照明电器有限公司、深圳市三和祥科技有限公司、广州国联通信有限公司、天津市北海通信技术有限公司、广州市源瑞信息科技有限公司、广州佳都智通科技有限公司、成都德源睿新科技有限公司、昊宇睿联（天津）科技有限公司、广州粤铁华启智能科技有限公司、广州铁科智控有限公司、四川省国有资产经营投资管理有限责任公司

本文件主要起草人：朱旻昊、彭金方、魏超、王建、钟飞、刘建华、贺继樊、戴兵刚、杨琦、李桂华、姜涛、贾鹏、韩冰、谭林、张建博、何晔、席文凯、张浩雨、殷桂明、胡涛、陈伟、黄海东、倪海忠、肖楠、王昊、侯亮勇、吴殿华、肖艳玲、杜立侠、金涛斌、冯波、何晶、孔祥云、齐幸辉、曾庆宁、马建荣、曾妮、李靓娟、钟文斌、刘化龙、谈沛婵、赵钧、董娜、曹丙胜、石彦夫、潘启兰、王涛、杨培、钟柳兴、于子飞、廖雯雯、刘长鸣、王平军、王振宇、赵贺飞、龙广钱、项学明

引言

本文件描述了城市轨道交通装备制造及其服务相关组织在可信性管理过程中建立可信性质量管理体系的要求。

本文件中，可信性是指城市轨道交通系统用于描述产品性能中与时间相关特性的术语。可信性是可靠性、可用性、可维修性、安全性（RAMS）和维修保障性的综合表述，并且包含装备的经济性，以全生命周期成本（LCC）衡量。

可信性建立信任和树立信心，并影响组织满足目标的能力，它可通过产品生命周期内有效的策划及实施可信性活动来获得。本文件中可信性将严重影响用户对于由组织开发或提供的产品或服务的价值的认知。可信性低将影响组织目标的实现并降低声誉。

可信性促进组织的技术改进、创新和产品的迭代更新。通过全生命周期过程获得的可信性可能受市场动态、世界经济和资源分配、用户需求的变化以及竞争性环境的影响。战略部署需要适应预期的变化，从而在商业运作中得以生存，可信性管理关注利益相关方通过优化可信性来提升组织的目标和投资回报。

本文件专门用于技术性的系统、产品、过程和服务，它们在本文件中进行描述时均使用通用术语“装备”或“产品”及其服务，标准中的大部分内容是通用的也可用于各种非技术性的应用。此外，当优化可信性时辨别、分析和管理安全性、环境和其他因素可能的影响。

城市轨道交通行业的市场准入，不仅要求装备或产品满足技术标准，也要求装备或产品在全生命周期内有质量和安全的保证。可信性管理的思想是在全生命周期内贯彻安全性、可靠性、可用性、可维护性、维修保障性和全生命周期经济性的协调发展。通过基于可信性质量管理体系标准的认证，可为城市轨道交通装备的市场准入的质量安全保证建立信任。

0.1 总则

建立可信性管理体系是组织的一项战略决策，能够帮助城市轨道交通行业提高全生命周期内的整体绩效，为推动可持续发展奠定良好基础。

组织根据本文件实施可信性管理体系的潜在益处是：

— 满足利益相关方的要求和目标；
— 实现期望的服务水平；
— 通过增加的可靠性提高企业产品核心竞争力；
— 通过增加的可用性保持生产或制造能力；
— 通过增加的维修性保证产品实际服役过程中的状态；
— 通过辨别并恰当地处理了潜在的有害影响，可提高安全性；
— 通过辨别并恰当地处理了有害影响，可减少环境影响；
— 通过技术迭代实现可信性整体水平的提升；
— 延长寿命和提高耐久性并减少全生命周期费用；
— 改善质量。

0.2 可信性管理是组织通用管理体系的一部分

可信性管理体系的目的是为了在可信性方面指导和控制组织，协同其他规程提供有效和整体的措施来实现目标。组织的方针和目标须包含可信性的方针和目标，然后，建立可信性管理体系来有效地实现。

图1说明了可信性管理是通用管理体系的一部分，可信性管理体系形成了可信性大纲并加入到组织的策划和活动中。

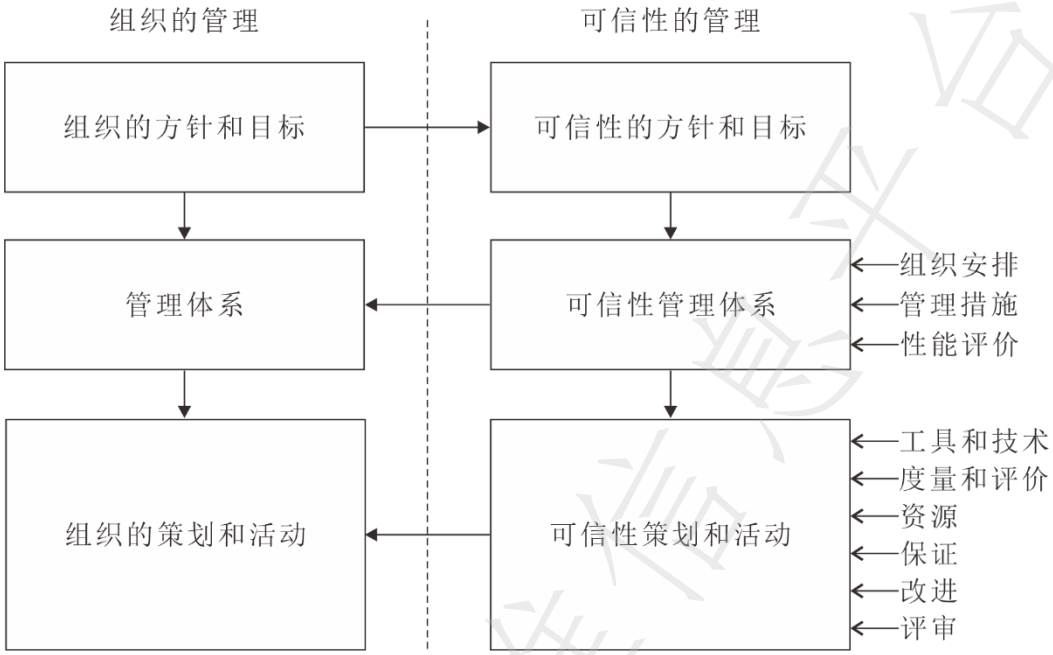

图 1　可信性管理体系与组织通用管理体系的关系

0.3　可信性管理与系统生命周期管理

0.3.1　可信性管理的时间相关性

可信性是一组与时间相关的性能的特性，通过系统的设计和实施来实现。可信性与质量、安全性、经济性和抗扰性等其他要求的特性共存。可信性与产品技术迭代和系统持续改进相关，无论是一个简单产品还是复杂的技术系统，其核心技术的发展都是遵循着客观的规律发展演变，即具有客观的进化规律和模式。

采用生命周期方法来获得可信性是实现可信性的关键。正确的设计和实施是成功运行的先决条件，可信性特性在生命周期的不同阶段（见图2）受到不同因素的影响，必须适当地加以管理。因此，可信性管理须贯穿于全生命周期管理的全过程。

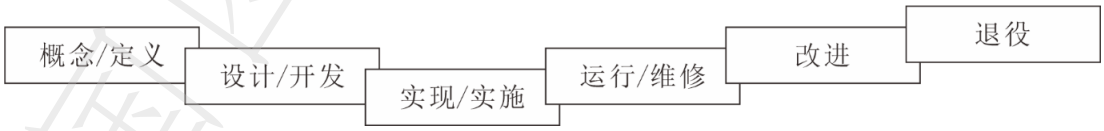

图 2　系统全生命周期过程

0.3.2　可信性管理的重要性

从城市轨道交通行业的角度来看，可信性管理对于组织的重要性在于：

— 可信性是商业合同和材料采购的关键决策因素；

— 可信性为全生命周期过程管理提供了战略框架；

— 可信性确保了产品或系统运行和维护的安全性、可靠性、可用性和完整性；

— 可信性原理和实践保障环境的可持续性，促进绿色环保技术应用；

— 可信性影响系统实现、资源分配和全生命周期费用；

— 可信性是资产管理的一个关键因素；

— 可信性方法支撑风险评估过程；
— 可信性可加快项目实施的成熟过程；
— 可信性倡导知识库的建立，通过失效及其后果的了解找到合适的解决方案来提高可信性；
— 可信性方针推动技术迭代演进和创新；
— 可信性应用关注技术管理支持和解决方案，提升系统全生命周期的经济性、组织过程的能力成熟度和资源的有效利用；
— 可信性可以向用户或业主传递信任，并获得客户的满意；
— 可信性支撑产品的品牌价值建立。

0.3.3 可信性管理与系统生命周期成本的关系

系统稳定的可信性水平决定了系统全生命周期成本。系统不可避免失效，系统在要求时不能有效运行，或安全、可靠运行，或系统的维修费用太高，不仅对组织的信誉带来不好的影响，用户可能会要求更换而不再维修，甚至出现客户流失；严重时可能导致灾难事故。另一方面，设计和制造一个高可信性的系统是昂贵的，以经济实用的价格生产这样一个系统是不可能的。因此，在低可靠的系统需要增加维修费用与高可靠的系统需要高昂的设计与制造费用两者之间进行权衡，系统不同可靠度与生命周期费用间关系见图3。

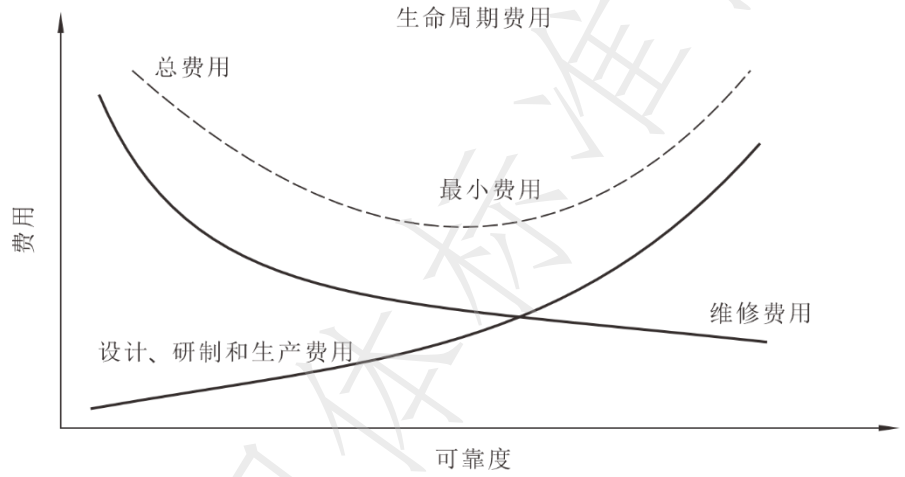

图 3 可靠度与系统生命周期费用的关系

0.4 运用基本概念和原则建立可信性管理体系

0.4.1 可信性管理体系

组织试图理解内、外部环境，以识别有关相关方的需求和期望。这些信息被用于可信性管理体系的建立，从而实现组织的可持续发展。一个过程的输出可成为其他过程的输入，并联结成整个网络。虽然不同组织的可信性管理体系，通常看起来是由相类似的过程所组成，但每个组织及其可信性管理体系都是独特的。

可信性管理体系是在ISO 9001（GB/T 19001）质量管理体系基础上建立，具有相同的基本构架。

可信性项目涉及系统生命周期的战略规划和技术应用。可信性项目涉及的活动包括但不局限于：

— 系统设计：用于实现功能特性的可信性；
— 项目管理和协调：用于确保过程实施的可信性；
— 知识库的开发和完善：用于支撑服务的可信性；
— 价值创造：用于保障技术转型的实现、产品的创新升级和技术迭代进步；

— 可信性保证：用于确保系统性能在运行中表现良好。

0.4.2 系统属性

系统为共同满足特定要求的相互关联要素的集合。一个系统包括硬件和软件、使用和维护系统的人员以及使用和维护系统的方法程序，同时，系统也包括其使用的环境。可信性规范应包括系统所有单元，因为系统任一单元的变化都将显著影响系统已达到的可信性水平。

系统的属性和相关性能特性见图4，性能特性表示最终用户感知或体验到的系统输出。特定的特性反映了所选的功能要求和非功能要求，这些要求应进行设计并纳入系统。系统的运行会受到外部因素影响，这些因素会影响系统性能。系统的影响条件域及其相关的影响因子域见图5。根据图4和图5的信息，可对给定条件和约束条件下的系统运行进行能力评估。

系统的类别和特征将影响系统可信性规范。例如，存在可修复和不可修复系统、一次使用设备；对于不可修复系统应更换而不是修理，其维修性和维修保障要求是完全不同的；对于一次使用设备，其正确量度是可靠度或者过早失效的概率。在编写可信性规范之前，采购方确保已充分辨识系统性质及其对可信性要求的影响。

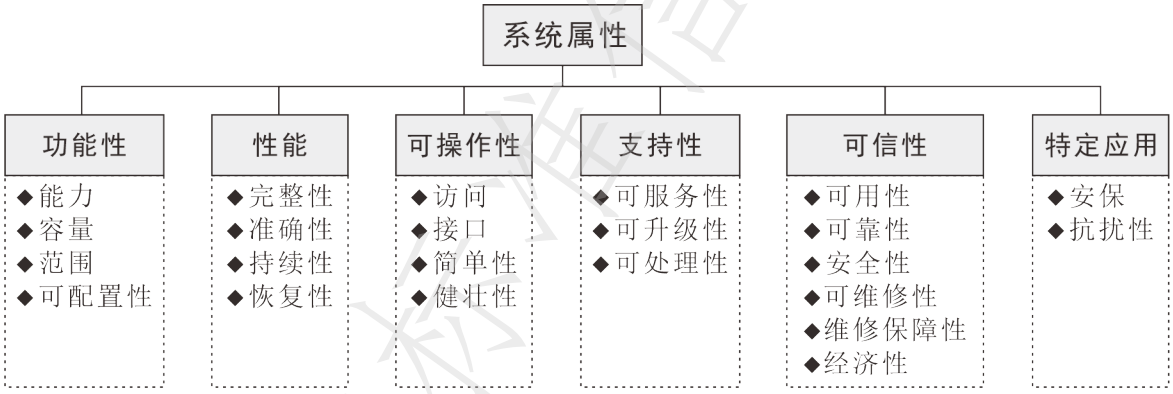

图 4 系统属性和相关的性能特性

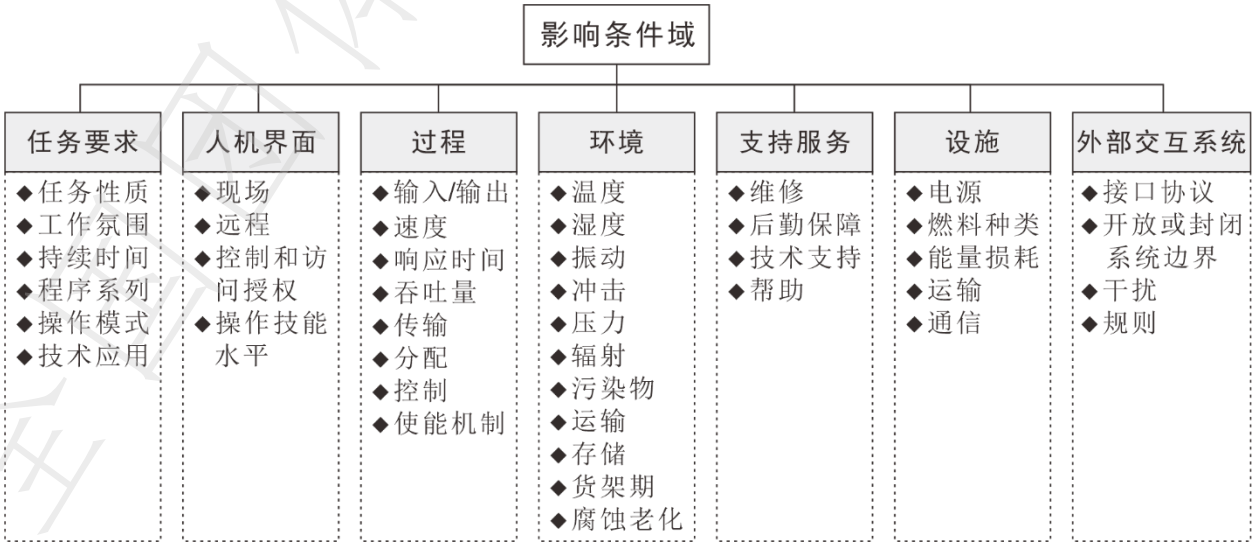

图 5 系统的影响条件域和相关的影响因子域

0.4.3 可信性管理

可信性管理提供系统的方法，用于解决可信性和来自于组织和商业远景的相关问题。可信性经常由技术驱动并结合老产品的技术迭代或演进。通过生命周期过程获得的可信性可能受市场动态、世界经济和资源分配、顾客需求的变化以及竞争性环境的影响。战略部署需要适应预期的变化，从而在商业运作中得以生存。可信性管理关注利益相关方通过优化可信性来提升组织的目标和投资回报。

可信性管理关注技术系统不同阶段的生命周期模型（见图6），根据具体的应用不同，可有不同的产品或系统描述。

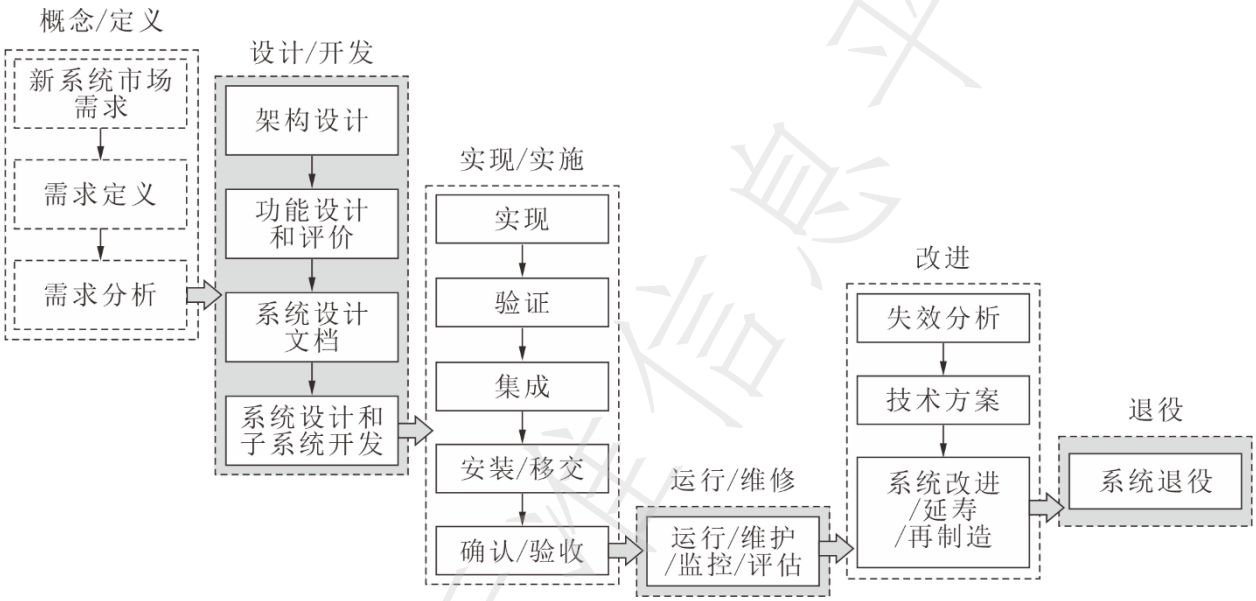

图 6　可信性管理过程的技术系统生命周期模型

可信性管理过程贯彻的是全生命周期管理的理念，必然要求持续改进实现系统或产品不断优化升级（见图7）。持续改进是一个不断循环迭代的过程，产品在整个生命周期内不可避免存在质量缺陷、性能衰退，甚至是失效、故障或事故。针对这些问题，需要通过一定的方法和流程，找出产生的原因，并在此基础上提出改进的技术方案。失效分析就是在全生命周期的技术迭代过程中，通过分析、模拟重现和验证，不仅要找出引起产品产生质量缺陷或性能衰退（即失效）的直接原因，而且要找出技术、管理方面的薄弱环节，并提出改进措施或防护方法。因此，失效分析是全生命周期持续改进过程的关键和必要环节或流程，是产品或产品技术迭代、质量提升的关键点，也是强化质量管理的必要手段和流程。

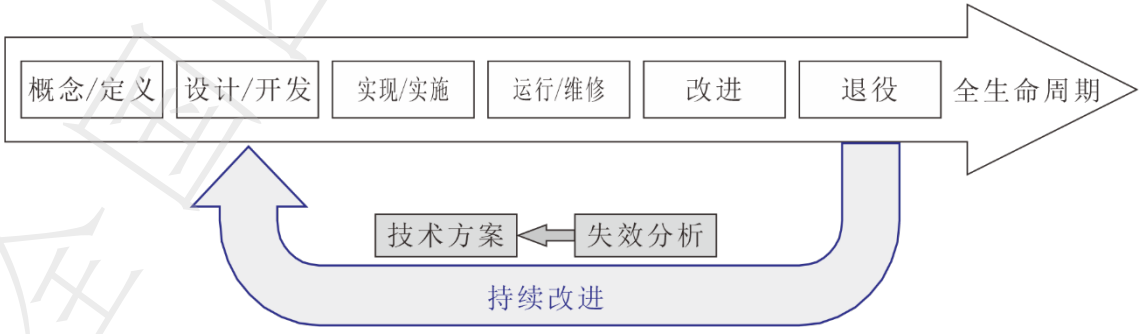

图 7　全生命周期管理中持续改进的实现路径

0.5　与其他管理体系标准的关系

本文件采用ISO制定的管理体系标准框架，以达到与其他管理体系标准的协调一致性。

本文件使组织能够使用过程方法，并结合PDCA循环和基于风险的思维，将其质量管理体系与其他质量管理体系标准要求进行协调或一致化。图8表明了本文件第4章至第10章是如何构成PDCA循环的。

PDCA循环可以简要描述如下：

——策划（Plan）：根据顾客的要求和组织的方针，建立体系的目标及其过程，确定实现结果所需的资源，并识别和应对风险和机遇；

——实施（Do）：执行所做的策划；

——检查（Check）：根据方针、目标、要求和所策划的活动，对过程以及形成的产品和服务进行监视和测量（适用时），并报告结果；

——处置（Action）：必要时，采取措施提高绩效，包括通过基于失效分析的技术方案使持续改进形成闭环管理系统。

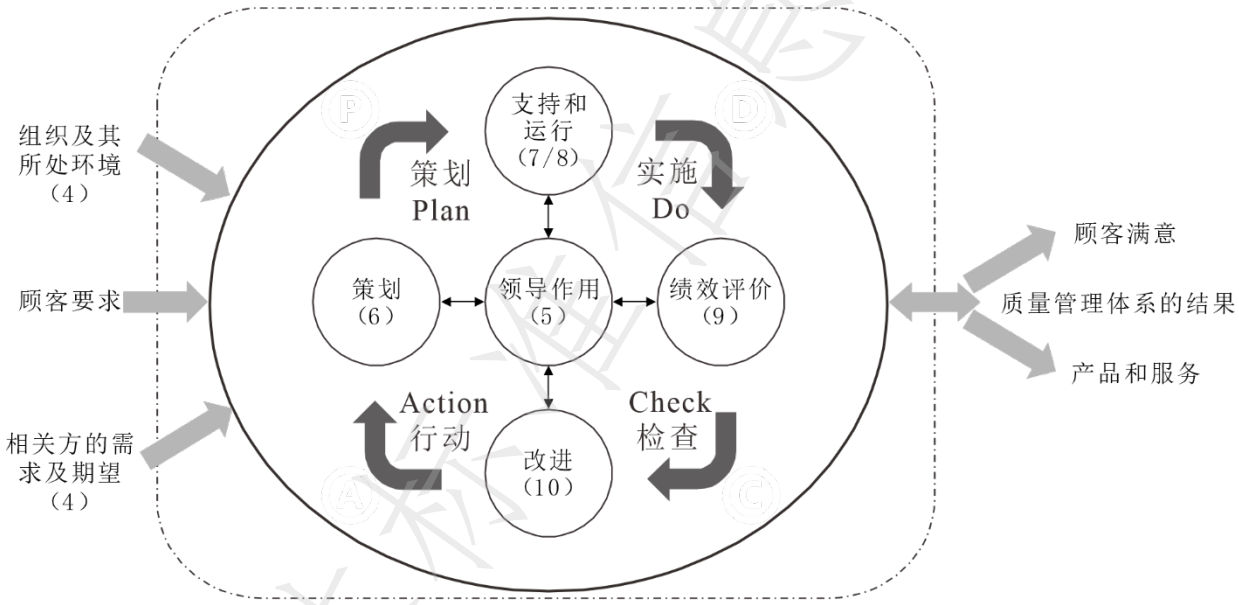

图 8　本文件的结构在 PDCA 循环中的展示（同 GB/T 19001）

本文件与GB/T 19000和GB/T 19001的关系是：

——GB/T 19000《质量管理体系 基础和术语》和GB/T 19001《质量管理体系 要求》为正确理解和实施本文件提供必要基础；本文件的第4章到第10章的目录结构（见图8）与GB/T 19001保持一致，是按PDCA循环展示可信性质量管理体系的要求。

本文件与ISO/TS 22163: 2023的关系是：

——本文件的制定参考了ISO/ 22163: 2023标准提供的铁路行业的管理体系要求。

城市轨道交通　装备可信性管理体系　要求

1　范围

1.1　本文件规定了城市轨道交通装备制造及其服务的组织的可信性管理体系要求以及城市轨道交通装备全生命周期从需求、设计、制造、装配、验收、服役、维修、改进/延寿/再制造和退役的全过程可信性管理的总体要求。

1.2　本文件适用于城市轨道交通行业从事产品的设计和开发、生产制造，以及维修维护、改进/延寿/再制造和退役等服务的组织的组织可信性管理和可信性管理体系认证，其他轨道交通系统的装备/产品及服务和机械装备行业的可信性管理可参考执行。

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 2900.99-2016 电工术语 可信性

GB/T 9414.1-2012 维修性 第1部分：应用指南

GB/T 9414.2-2012 维修性 第2部分：设计和开发阶段维修性要求与研究

GB/T 9414.3-2012 维修性 第3部分：验证和数据的收集、分析与表示

GB/T 9414.5-2018 维修性 第5部分：测试性和诊断测试

GB/T 9414.9-2017 维修性 第9部分：维修和维修保障

GB/T 19000-2016 质量管理体系 基础和术语

GB/T 19001-2016 质量管理体系 要求

GB/T 36615-2018 可信性管理 管理和应用指南

GB/T 36657-2018 可信性管理应用指南可信性要求规范指南

GB/T 39844-2021 可靠性增长 统计试验和评估方法

GB/T 21562-2008 轨道交通 可靠性、可用性、可维修性和安全性规范及示例

GB/T 21562.2-2015 轨道交通 可靠性、可用性、可维修性和安全性规范及示例 第2部分：安全性的应用指南

GB/T 21562.3-2015 轨道交通 可靠性、可用性、可维修性和安全性规范及示例 第3部分：机车车辆RAM的应用指南

ISO 22163: 2023 Railway applications — Railway quality management system — ISO 9001:2015 and specific requirements for application in the railway sector

3　术语和定义

GB/T 19000-2016和GB/T 2900.99-2016界定的以及下列术语和定义适用于本文件。

3.1

术语

3.1.1

组织 organization

为实现目标（3.1.6），由职责、权限和相互关系构成自身功能的一个人或一组人。

注1：组织的概念包括: 从事城市轨道交通产品设计和开发、生产制造，以及维修维护、改进/延寿/再制造和退役等服务的法人或非法人组织。

注2：这是ISO／IEC导则，第1部分的ISO补充规定的附件SL中给出的ISO管理体系标准中的通用术语及核心定义之一，最初的定义已经通过修改注1被修订。

注3：如果组织是大型实体的某个组成部分，那么，术语“组织”仅指在可信性管理体系（3.1.4）范围内的这个组成部分。

3.1.2

相关方 interested party

能够影响决策或活动、受决策或活动影响或自认为受决策或活动影响的个人或组织（3.1.1）。

3.1.3

最高管理者 top management

在最高层指挥和控制组织(3.1.1)的一个人或一组人。

注1：最高管理者有权在组织内部授权和提供资源。

注2：如果管理体系(3.1.4)的范围仅覆盖组织的某个组成部分，那么最高管理者是指挥和控制该部分的一个人或一组人。

3.1.4

管理体系 management system

组织(3.1.1)为确立方针(3.1.5)和目标(3.1.6)以及实现这些目标的过程（3.1.7)所形成的相互关联或相互作用的一组要件。

注1：一个管理体系可能针对一个或几个主题。

注2：管理体系要件包括组织的结构、岗位和职责、策划和运行。

3.1.5

方针 policy

由最高管理者(3.1.3)正式表述的组织(3.1.1)的意图和方向。

3.1.6

目标 objective

要实现的结果。

注1：目标可能是战略的、战术的或运行的。

注2：目标可能涉及不同的主题(如财务、健康、安全和环境)。它们可能存在于不同层面。诸如组织整体层面或项目、产品或过程(3.1.8)层面。

注3：目标能够用其他方式表述，如：预期的结果、宗旨、运行准则，可信性目标或使用其他有类似含义的词(如：终点或指标)。

注4：在可信性管理体系(3.1.4)中，组织(3.1.1)设定的可信性目标与可信性方针(3.1.5)保持一致，以实现特定的结果。

3.1.7

风险 risk

不确定性的影响。

注1：影响是对预期的偏离——正面的或负面的。

注2：不确定性是一种状态，是指对某个事件、事件的后果或可能性缺乏甚至部分缺乏相关信息、理解或知识。

注3：通常，风险以潜在事件(见GB/T 23694-2013中的定义，4.5.1.3)和后果(GB/T 23694-2013中的定义4.6.1.3)或二者的组合来描述其特性。

注4：通常，风险以某个事件的后果(包括情况的变化)及其发生的可能性(见GB/T 23694-2013中的定义4.6.1.1)的组合来表述。

3.1.8

过程 process

使用或转化输人以实现结果的一组相互关联或相互作用的活动。

注：某个过程的结果是称为输出,还是称为产品或服务，取决于相关语境。

3.1.9

能力 competence

应用知识和技能实现预期结果的本领。

3.1.10

顾客 customer

能够或实际接受为其提供的，或应其要求提供的产品或服务的个人或组织。示例，消费者、委托人、最终使用者、零售商、内部过程的产品或服务的接收人、受益者和采购方。

注：在本文件中，顾客可以是产品采购方，如采购零部件的生产制造组织、采购产品的运营组织等，也可以是服务接受方，如接受运营服务的乘客、接受维修及其他服务的运营组织等。

3.1.11

供方 provider (supplier)

提供产品（3.1.12）或服务（3.1.13）的组织（3.1.1)。示例：产品或服务的制造商、批发商、零售商或商贩。

注1：供方可以是组织内部的（内部供方）或组织外部的（外部供方）。

注2：在合同情况下，供方有时称为“承包方”。

3.1.12

（城市轨道交通）装备 equipment, <of an item>

城市轨道交通领域为完成特定任务或目标所需配备的各种工具、器械、设施、系统等的总称。城市轨道交通装备包括机车车辆、工程建设与养护机械、通信信号设备、安全保障设备（如：屏蔽门、监控系统、消防系统）、牵引供电设备、运营管理设备等，用于保障交通系统的正常运行和乘客的安全舒适。

3.1.13

产品 product

在组织（3.1.1)和顾客（3.1.10）之间未发生任何交易的情况下，组织（3.1.1)能够产生的输出。

注1：在供方和顾客之间未发生任何必要交易的情况下，可以实现产品的生产。但是，当产品交付给顾客时，通常包含服务因素。

注2：通常，产品的主要要素是有形的。

注3：硬件是有形的，其量具有计数的特性（如：车轮）。流程性材料是有形的，其量具有连续的特性（如 燃料和润滑剂）。硬件和流程性材料经常被称为货物。软件由信息组成，无论采用何种介质传递（如：计算机程序、移动电话应用程序、操作手册、字典、驾驶执照）。本文件中的产品包括了硬件和软件，以及由它们集成的系统。

3.1.14

（轨道交通领域）服务 service，< in railway field>

至少有一项活动必须在组织（3.1.1)和顾客（3.1.10）之间进行的组织的输出。

注1：通常，服务的主要特征是无形的，由顾客体验。

注2：通常，服务包含与顾客在接触面以确定顾客要求的活动，除提供服务外还可能涉及建立持续的关系，如：提供城市轨道交通产品维护维修服务、计量检测、失效分析等的组织等。

注3：服务的提供可能涉及，例如：

— 在顾客提供的有形产品（如需要维修的城市轨道车辆、设备）上所完成的活动。
— 无形产品的交付（如提供城市轨道交通产品相关知识的培训）。

注4：本文件中指运营单位为保障城市轨道交通装备的安全、可靠、高效、经济的运行，提供的各种设施设备的运行维护、更新改造、技术管理等。

3.1.15

文件化信息 documented information

组织(3.1)需要控制和维护的信息及其载体。

注1：文件化信息能够以任何形式和载体存在，且来源不限。

注2：文件化信息可能涉及：

— 管理体系(3.1.4)，包括相关过程(3.1.8)；
— 为组织运行而创建的信息(文件)；
— 实现的结果的证据(记录)。

3.1.16

绩效 performance

可测量的结果。

注1：绩效可能涉及定量的或定性的结果。

注2：绩效可能与活动、过程(3.1.8)产品服务体系或组织(3.1.1)的管理有关。

3.1.17

持续改进 continual improvement

提高绩效(3.1.16)的循环活动。

注1：通过不断地进行变革、创新和提高，实现某一或某些运营过程、产品和服务等的不断发展和进步。这是一个涉及持续规划、监控、实施和纠正可能出现的问题的过程。持续改进要求组织营造一个全员参与、主动实施改进的氛围和环境，以确保改进过程的有效实施。

注2：不仅是质量管理的一个重要原则，也是组织追求永恒目标的一种表现。持续改进的目的是增加顾客和其他相关方的满意度，提高过程和体系的有效性、效率及整体业绩。

3.1.18

有效性 effectiveness

完成策划的活动和实现策划的结果的程度。

3.1.19

要求/需求 requirement

规定的、不言而喻的或有义务履行的需要或期望。

注1：不言而喻的或有义务履行的需要或期望是指需求。其中，“不言而喻”是指组织(3.1.1)和相关方(3.1.2)的惯例或一般做法，不言而喻的需要或期望是不用说就明白的。

注2：规定的需要或期望是指要求，也就是符合GB/T 1.1中定义的要求，即表达声明符合该文件需要满足的客观可证实的准则。

3.1.20

可信性 dependability

指系统需要时按要求执行的能力。是系统的固有属性，适用于任何涉及硬件、软件和人员方面的系统、产品、过程或服务。

注1：可信性包括可靠性、可用性、可维修性、安全性、维修保障性和全生命周期经济性，以及在某些情况下，诸如耐久性和安保等其他特性。

注2：可信性是用于产品与时间相关质量特性的集合性术语。

[来源：GB/T 2900.99-2016,定义192-01-22,有修改]

3.1.21

可信性管理 dependability management

在可信性方面指导和控制组织的协调活动。

注：可信性管理是组织整体管理的一部分。

3.1.22

可信性管理体系 dependability management system

组织的一组相互关联或相互作用的要素，用于建立可信性的相关方针、目的以及实现可信性目的的过程。

注1：管理可信性的体系是整体管理体系的一部分，一般来说，它不是一个单独的管理体系。

注2：体系要素包括组织的结构、角色与职责、策划、程序和过程。

3.1.23

可信性计划 dependability plan

为了实现产品可信性目的和目标的一组有计划的活动。

3.1.24

可信性大纲 dependability program

经济高效地实现可信性目标的活动以及资源配置的一组协同计划。

3.1.25

（产品的）可靠性 reliability, <of an item>

装备或产品在给定的条件下，给定的时间区间内，能无失效地执行要求（完成规定功能）的能力。

注1：持续时间区间可用装备有关的适合的计量单位表示，例如日历时间、运行周期行程等，这些计量单位宜清晰的阐述。

注2：给定的条件包括影响可靠性的各个方面，如：运行模式、服役条件、环境条件（如温度、湿度、辐射、磁场、电场、冲击、振动等及其组合）、失效模式和维修等。

注3：可靠性采用适当的量度予以定量化。

注4：规定功能是对产品故障规定判断的依据，常用产品的各种性能指标来描述产品的功能。

注5：能力是各种可靠性指标，这些指标是对可靠性的定量描述，以便说明产品可靠性的程度。

[来源：GB/T 2900.99-2016,定义192-01-24,有修改]

3.1.26

安全 safety

防止发生不可接受的风险的损害。

3.1.27

（产品的）安全性 safety , <of an item>

装备或产品所具有的不导致人员伤亡、系统毁坏、重大财产损失或不危及人员健康和环境的能力。安全性是各类装备都具有的一种固有属性，与可靠性、维修性和维修保障性等密切相关，是各种产品必须满足的首要设计要求，是通过设计赋予的产品属性。

3.1.28

(产品的)可用性 availability, <of an item>

在某个考察时间，系统能够处于按要求执行规定功能的能力。它是衡量产品在投入使用后实际使用的效能。

注1：可用性取决于产品可靠性、恢复性、维修性的综合特征。

注2：可用性采用适当的量度予以定量化。

3.1.29

维修

3.1.29.1

维修 maintenance

为保持或恢复产品处于能完成要求功能的状态而进行的所有技术和管理活动的组合。

3.1.29.2

(产品的)可维修性 maintainability, <of an item>

在给定的使用和维修条件下，保持或恢复能执行规定功能的状态的能力。

注1：给定的条件包括影响维修性的各个方面，如：维修场所、可达性、维修程序和维修资源。

注2：维修性采用适当的量度予以定量化。

注3：根据维修工作的需要，装备或产品可按划分的“维修约定级”进行阶梯差异化维修。

3.1.29.3

维修保障 maintenance support

维修产品的资源的供给。

注：资源包括人力资源、保障设备、材料和备件、维修设施、文档和信息以及维修信息系统。

3.1.30

（产品的）生命周期

3.1.30.1

（产品的）生命周期；寿命周期 life cycle,<of an item>

产品从需求提出开始，经历设计、制造到运行、服务和改进、处置的整个周期的时间。

示例：典型的系统生命周期包括：概念和定义；设计和开发；实现和实施（即制造、安装、试运行和验收等）；运行和维修；改进（包括寿命期技术升级或延寿或再制造）；退役和废弃。

注：划分的阶段将根据实际应用而变化。本文件未对“生命周期”和“寿命周期”两个词语做严格区分。

3.1.30.2

（产品的）生命周期费用；（产品的）寿命周期费用 life cycle costing，< of an item >

在生命周期内发生的总费用，简写为LCC。经济分析的过程，以评估一个项目在其整个生命周期或其中一部分的费用。

3.1.30.3

概念和定义阶段 concept and definition stage

产品生命周期中定义和识别运行使用环境和时间线，初步定义系统要求，和(通常)规定产品规范的阶段。

3.1.30.4

设计和开发阶段 design and development stage

在产品生命周期中计划或执行选取的工程设计方案，以实现系统功能的阶段，也是形成产品的硬件和/或软件以及编制硬件的详细制造规范、软件的编写规范和其他产品文件(如维修保障计划、使用和维

修说明书、操作规程等)的阶段。设计活动包括架构设计、功能设计和评价，开发活动包括系统及子系统要素的详细设计数据和功能接口信息，以及工程建模、原型构造、风险评估和接口识别等。

3.1.30.5

实现和实施阶段 achievement /implementation stage

在产品寿命周期中实现阶段应开展技术应用、制造、包装和寻找供应源等活动，获取和部署子系统要素，确保从系统设计到特定产品或子系统要素的完全转变的阶段。该阶段的关键过程活动包括：实现，以硬件和软件形式构成系统和子系统的要素；验证，确认系统满足特定的设计要求；集成，组成与架构设计配置一致的系统和子系统；安装/移交，配置系统性能，提供在特定操作环境中所需的性能服务；确认/验收，提供满足系统功能、性能要求的客观凭证。

3.1.30.6

运行和维修阶段 operation and maintenance stage

在产品生命周期中使用产品并进行维修和保障的阶段。该阶段该阶段的关键过程活动包括：运行，展现系统交付能力，完成预期的功能要求贺服务；维修，保持性能并处理服务的失效和中断；监控，验证系统性能和效果改进，确保可信性和服务质量目标得到满足。

3.1.30.7

改进阶段 Improvement stage

在产品生命周期中通过增加特性提升系统性能，满足系统不断增长和变化的顾客需求的阶段。在该阶段，针对系统性能退化或失效，以及不断提高的顾客需求，利用故障诊断/失效分析方法，找出性能退化或失效机理，提出技术改进的解决方案，以实现技术迭代和系统演进，达到增加或改善系统特性的作用。在该阶段，也可以通过技术解决方案，实现产品延寿和产品再制造的重复利用。

3.1.30.8

退役阶段 Decommissioning stage

在产品生命周期中终止系统存在的阶段。在该阶段，系统可能被拆解、重新部署用于其他服务，或者在不影响环境的情况下在相应的地方被处理。处置过程需要考虑硬件的剩余价值并支持可持续性。

3.1.31

（过程的）剪裁 tailoring

适应、调整或改正组织的一套已建立的过程和活动，以实现、符合或满足可信性要求的过程。剪裁过程应用于管理过程、项目活动和管理评审，可应用于系统全生命周期的任何一个阶段。

3.1.32

失效与故障

3.1.32.1

（产品的）故障 fault，< of an item >

产品不能执行规定功能的状态。所指状态如短路、开路、漏油、网络故障等。

3.1.32.2

（产品的）失效 failure，< of an item >

装备或产品丧失规定功能的能力的事件。

注1：失效包括完全丧失其功能、部分失去功能（虽然能够工作，但不能完成规定功能）和不能确保安全可靠工作（虽然能够完成规定功能）等情况。装备或产品在服役过程中的性能退化是失效的表现形式。

注2：“故障”表明的是一种状态，而“失效”则是一个事件，本文件中，两个词语未做严格意义的区分。

3.1.32.3

失效模式 failure mode

失效发生的种类。

注1：失效模式可由功能丧失或发生其他状态的转变来规定。

注2：失效模式按突发性分为突然失效和渐变失效；按出现的时间分为早期失效和晚期失效；按失效原因分为正常损耗、本质缺陷、误用和超负荷失效；按失效机理分为结构失效、热失效、电失效和腐蚀失效。

3.1.32.4

失效分析 failure analysis

根据失效/故障模式和现象，通过分析、模拟重现和验证，识别失效/故障或非期望事件产生原因的系统过程，并对产生的后果、影响范围、发生概率等进行系统科学、客观的分析，其中包括找出技术、管理方面的薄弱环节，以便通过设计、过程或程序的变更等技术解决方案，提出使其消除或改进措施的方法。

注：本文件中，失效分析的内涵大于故障分析，失效分析包含了故障分析。

3.2 缩写词

CA	购置成本(Cost Of Acquisition)
CD	废置处理成本(Cost of Disposal)
CF	失效成本(Cost Of Failure)
CFA	失效分析成本(Cost of Failure Analysis)
CM	养护维修成本(Cost of Maintenance)
CO	运行成本(Cost of Operation)
EPPPS	外部提供的产品、过程或服务（External Provisioned Products, Processes, or Services）
ERP	企业资源计划管理系统(Enterprise Resource Planning)
FAI	首件检验（First Article Inspection）
FMEA	失效/故障模式及影响分析(Failure Mode and Effects Analysis)
FMECA	失效/故障模式影响及危害性分析(Failure Mode, Effects, and Criticality Analysis)
FRACAS	失效/故障报告、分析和纠正措施系统(Failure Reporting, Analysis, and Corrective Action System)
KPI	关键绩效指标(Key Performance Indicator)
LCC	生命周期成本(Life Cycle Cost)
MAMT	平均有效维修时间(Mean Active Maintenance Time)
NPV	净现值(Net Present Value)
PDCA	策划–实施–检查–处置(Plan-Do-Check-Act)
PHM	（失效/故障）诊断与健康管理系统(Prognostics and Health Management)
QDC	质量缺陷成本(Quality Defect Cost)
RAM	可靠性、可用性、可维修性(Reliability, Availability, Maintainability)
RAMS	可靠性、可用性、可维修性、安全性(Reliability, Availability, Maintainability,safety)
RCMA	可靠性为中心的维修分析(Reliability-Centered Maintenance Analysis)
SIL	安全完整性等级(Safety Integrity Level)
TRL	可信性等级
WBS	工作分解结构(Work Breakdown Structure)

4 组织环境

4.1 理解组织及其环境

4.1.1 组织应符合 GB/T 19001-2016 中 4.1 和 ISO 22163:2023 中 4.1.1、4.1.2 的要求。

4.1.2 组织应确定与可信性管理相关的集体、过程、方法、技术的策划和应用,以实现组织的性能和产品目标。

4.1.3 组织应确定与可信性管理相关的因素及其影响，包括但不限于：相关技能资源可用性和可获取性、项目风险、供应链能力、投资回报、管理约束等。

4.1.4 组织应确定与可信性活动成功实现的关键因素，包括：

a）规定单独的整体责任，以满足可信性要求并协调涉及的各种组织实体之间的共同责任；

b）管理与可信性及相关的功能要求有关的信息；

c）协调涉及可信性活动的内部和外部小组；

d）明确和量化组织的可信性目标；

e）制定和执行可信性策略；

f）开展和改进可信性的验证。

4.2 理解相关方的需求和期望

4.2.1 组织应符合 GB/T 19001-2016 中 4.2 的要求。

4.2.2 组织应确定城市轨道交通产品可信性管理的利益相关方，包括顾客、供应商、操作人员、维修人员等以确保可信性要求得以满足

4.2.3 组织应确定利益相关方对产品的可信性需求，包括产品的功能要求与非功能要求。

4.3 确定可信性管理体系的范围

4.3.1 组织应符合 GB/T 19001-2016 中 4.3 和 ISO 22163:2023 中 4.3.1 的要求。

4.3.2 组织应确定产品随生命周期发展过程中各生命周期阶段转换所需的技术资源、多元化的授权体系和支撑准则。

4.3.3 组织在确定可信性管理体系的范围时，还应考虑：

a） 覆盖组织所有关键的部门和流程，确保整个组织内的活动和资源都得到适当的考虑和管理。

b） 与产品全生命周期相关并由其他组织实施的可信性活动的接口及边界。

c） 根据利益相关方的需求和期望，确定需要满足的可信性管理要求的范围。

4.4 可信性质量管理体系及其过程

组织应符合GB/T 19001-2016中4.4.1、4.4.2和ISO 22163:2023中4.4.3的要求。

4.4.1 可信性要求

4.4.1.1 可信性要求规范

组织应明确编制城市轨道交通产品及其服务的相关方的可信性要求规范，应包括：

a） 定性的产品可靠性和维修性要求、产品功能、故障判据、环境和运行条件、符合预期要求的产品寿命的规定；

b） 可靠性、维修性和可用性等性能（例如总失效率、任务可靠性、平均不工作时间）测量的定量要求；

c） 测试性要求（测试功能和程序、各个产品级别的测试精度等）；

d） 维修保障的定性和定量要求（或条件）。

注：相关方可为产品的制造商、供应商、运营方/用户等。

可信性要求规范应具有明确性、可验证性、一致性和可追溯性。每个要求的规定也应说明必须进行一致性检验的方法和程序（分析方法、仿真、测试等）以及生命周期阶段。

4.4.1.2 可信性要求说明

组织应具备城市轨道交通产品可信性要求说明的相关文件化信息，并附在可信性要求规范之后，要求说明应包括对产品预期的用途以及会影响其可信性的条件和约束的分析：

a） 运行和维修条件，包括任务类型和持续时间；
b） 确认预期用途中产品的工况；
c） 在使用的每一个阶段以及维修和保障活动期间，确定产品的部件或组件的环境和运行条件；
d） 确定人为、环境、技术和时间因素的影响；
e） 确定制造、试验、贮存包装、运输、搬运和维修的影响；
f） 确认由于维修方针、个人技能水平等引起的约束，并适时提出更改建议。

4.4.1.3 可信性要求分配

组织应对设计、运行和维修活动中对产品及其服务的可信性要求进行验证和确认，把可信性要求分配给产品的各个子系统、组件和部件。

注1：对产品及其部件进行可信性要求分配应符合GB/T 36657-2018所规定的内容。

注2：在分配可信性特征量时，对产品的某些零部件和某生命周期阶段来说，可能有必要使用其它方法而不是可信性规范中规定的方法(例如在计和开发阶段的可靠性控制中，可使用在各项试验活动中发现的故障数目)作为判定准则。

最终，产品的任何系统或零部件的规范中都应包含所分配的可信性要求，并将其用作验证、确认和试验程序的规定和设计的基础。

4.4.1.4 可信性保证

组织应建立文件化的产品可信性保证策略和实施方法，可信性保证过程应包含：

a） 在规定时间内，通过产品在其所属应用环境中的实际使用情形来证明其可信性，包括正式的演示或在保修/工作期间的实际性能；
b） 针对构成产品可信性的数据，利用统计方法推测出可信性；
c） 提供正确实施了要求的可信性活动的证据。

4.4.2 生命周期费用大纲

组织应按本文件的要求建立产品生命周期费用大纲。通过对大纲的分析，生命周期费用分析程序应在产品交付前的每一生命周期阶段实施并完成。分析的结果应用于管理决策过程，以：

a） 指导各种可信性要求之间的分配与权衡，例如灵敏度分析；
b） 确认对寿命周期成本起关键作用的可信性因素；
c） 对各种设计和保障方案的选择进行指导；
d） 优化在生命周期费用约束条件下的可信性；
e） 选择产品处置方法。

为了完成生命周期费用所需的计算，供方应要求用户提供其正在策划的维修保障条件和特性。

组织应形成文件化信息，以指导产品全生命周期费用计算与分析，分析过程应包含：

a） 准备适用成本的细分结构；
b） 确定每个细分要素的成本；

c） 从行业来源或实际经验中收集的失效数据和修理数据；
d） 分析系统的可用性和可靠性；
e） LCC模型，例如，LCC= CA+ CO + CM+ CF+ CD - NPV；
f） LCC模型每个组件的预估成本；
g） 在研究期间使用折扣情况；
h） 基于净现值（NPV）确定最终LCC的过程。

4.5 可信性管理体系的融合

组织建立的可信性管理体系应与组织的质量管理体系融合形成一个完整的管理体系制度，以提高组织的整体质量水平和竞争力。融合过程应符合：

a） 策划阶段（即概念和定义阶段）：组织应明确可信性需求和质量目标，并将其转化为具体的指标和标准，作为设计、实现和评估的依据。同时，应制定可信性管理计划和质量管理计划，并将其整合为一个统一的管理计划，明确各个阶段的任务、责任、资源、方法和工具。
b） 设计和开发阶段：组织应采用符合可信性原则和质量要求的设计方法和技术，如模块化、抽象化、正交化、冗余化等，以提高软件或系统的安全性、可靠性、可维护性等属性。同时，应该对设计结果进行可信性分析和质量评审，并根据反馈进行改进。
c） 实现和实施阶段：组织应遵循可信性规范和质量标准，如编码规范、测试规范等，以保证软件或系统的正确性、一致性、完整性等特征。同时，应该对实现结果进行可信性测试和质量检验，并根据结果进行修正。
d） 运行和评估阶段：组织应采用符合可信性评价和质量审核的方法和工具，如可信度模型、度量指标、审计程序等，以验证软件或系统是否满足可信性需求和质量目标。同时，应该对评估结果进行总结和报告，并提出改进建议。
e） 维修和改进阶段：组织应建立可信性监控和质量保障的机制和流程，如故障报告、故障诊断、失效分析、故障恢复、故障预防、维修、延寿等，以保持软件或系统的正常运行和持续改进。同时，应该定期对软件或系统进行可信性复核和质量复审，并根据反馈进行升级。

5 领导作用

5.1 领导作用和承诺

5.1.1 组织应符合 GB/T 19001-2016 中 5.1.1 和 5.1.2 的要求。
5.1.2 最高管理者还应通过以下内容，证实其对可信性管理体系的领导作用与承诺：

a） 为实现可信性目标和降低管理风险而采取的可操作的计划和控制手段；
b） 通过辨别可信性要求和问题、传达可信性大纲状态、解决和平衡冲突以保护和维护协议和问责制等环节，使各利益相关方介入；
c） 协调不同的组织职能，这涉及到可信性活动，以及为协调管理和技术活动的可信性责任分配；
d） 为可信性目的和目标管理风险；
e） 为实现可信性，管理产品生命周期内所需的技术活动；
f） 确保可信性管理体系所需的资源可获得，并有效地分配和利用；
g） 确保可信性管理体系实现其预期结果，并及时监测、评价、审核和报告其绩效。

5.2 方针

组织应符合GB/T 19001-2016中5.2.1、5.2.2和ISO 22163:2023中5.2.3的要求。

5.2.1 可信性方针

组织建立可信性方针应：

a) 作为可获取的文件化信息；
b) 在组织内予以沟通；
c) 视情况可被相关方获取；
d) 与组织的方针以及利益相关方的技术和商业远景保持一致；
e) 可作为组织的质量方针的组成部分；
f) 阐述失效/故障预防、基于技术解决方案的技术迭代或改进，以及满足及超越顾客期望的理念。

5.3 组织内的岗位、职责和权限

5.3.1 组织应符合 GB/T 19001-2016 中 5.3 和 ISO 22163:2023 中 5.3.1、5.3.2 的要求。

5.3.2 最高管理者设置管理岗位、分配职责和权限时，还应考虑：

a) 设置负责可信性工作的岗位，并赋予相应的职责和权限，该岗位可以是独立的或作为其他角色的一部分；
b) 各管理岗位相关人员应具备相关的专业知识、技能和经验，能够对城市轨道交通系统的可信性进行分析、评估、监测和改进，以及对可信性相关的风险进行识别、评估和控制；
c) 能与城市轨道交通系统的全生命周期各个阶段和部门进行有效的沟通和协调，确保可信性要求和目标在各个环节得到落实和满足；
d) 可信性管理岗位以及相关职责、权限等与组织的背景、目标、战略以及风险和机遇相适应；
e) 可信性管理体系宜与组织其他的管理体系进行融合，形成一个完整的管理体系制度；
f) 与可信性活动相适宜的结构和报告等级制度；
g) 可信性管理岗位以及相关职责、权限的设定应有助于可信性决策制定，并引领技术发展。

6 策划

6.1 应对风险和机遇的措施

组织应符合GB/T 19001-2016中6.1.1、6.1.2和ISO 22163:2023中6.1.3、6.1.4的要求。

6.1.1 可信性风险管理

6.1.1.1 风险评估

为切实降低成本，减少不良后果产生的影响，对产品而言组织应在实现其要求与提高性能的机会中辨别潜在的风险，并进行风险评估。辨别过程中要综合考虑关于可信性、功能和非功能目标（如安全性或环境需求）的风险。组织应：

a) 从设计、制造、试验、安全、运营、维修、改进等方面出发，建立一个结构化的风险评估和管理流程，从而对产品全生命周期过程进行风险评估；
b) 通过建立智能化数据分析技术以及数据监测平台，分析产品运行数据状态，以检测产品使用过程中的潜在的风险；
c) 安排人员对外部环境进行监视，从而获得关于变化的早期预警；
d) 考虑规定要求、活动和计划来满足产品恢复并适应风险的需要。

6.1.1.2 风险管理过程

组织应通过采用一般的风险管理过程来处理风险，风险管理过程应包括：

a) 定义风险相关的可信性问题；

b） 识别风险；
c） 进行风险分析；
d） 进行失效分析。

在产品全生命周期的各个阶段，风险分析和失效分析应有负责该阶段的主管部门来进行，并形成文件化信息。该文件至少应包括：

a） 分析方法及方案；
b） 方法的假设、限制和判据；
c） 危害鉴定结果及责任划分；
d） 风险或失效的评估结果和置信度水平；
e） 平衡研究的结果；
f） 数据及其来源与置信度水平；
g） 实施风险评价和失效分析评价；
h） 确定风险处理或失效分析技术解决方案，并对其有效性进行验证或确认；
i） 审查风险和失效问题解决的充分性；
j） 在风险管理过程中的风险和失效的相关信息和技术专家的建议。

6.1.1.3 失效风险评估

由于产品在运行时失效，可能导致对人的伤害和巨大的经济损失，组织应进行失效风险分析，应包括：

a） 确定产品研制过程中可能导致失效的风险源，包括技术风险、管理风险、环境风险等；
b） 对风险源所造成的失效后果进行定性或定量的分析，确定风险的严重性、发生概率和可控性；
c） 对风险控制措施的执行情况进行跟踪和评价，检查风险是否得到有效控制或消除，并及时调整风险控制策略；
d） 根据风险值的大小，制定相应的风险控制措施。

6.2 可信性目标及其实现的策划

6.2.1 质量目标

组织应符合GB/T 19001-2016中6.2.1的要求。

6.2.2 质量目标实现的策划

组织应符合GB/T 19001-2016中6.2.2的要求。

6.2.3 可信性目标

6.2.3.1 可信性目标的活动

组织应建立产品在全生命周期中的可信性目标，以明确定义和特定产品有关的用户可信性要求，应完成以下活动：

a） 识别客户、所关注的系统和应用环境；
b） 阐明组织对客户需求和要求的理解；
c） 确定项目责任，明确项目负责人和已分配的项目团队人员；
d） 确定项目持续期内的预算计划和资源需求；
e） 列出工作清单、计划和完成目标的日期；
f） 概述系统要求背景下可信性解决方案的技术途径；
g） 为可信性活动的及时实施提供特定的资源；
h） 识别外包需求和优选供应商的名录指南；

i） 能够测量可信性的进展状态；
j） 在适当情况下进行风险评估，减少暴露并降低潜在风险；
k） 评审可信性输出结果，用于评估项目任务的完成情况，以及需要进一步关注的缺陷；
l） 在需要时为持续改进做出适当改变；
m） 建立用户接口和供应链协作；
n） 确保系统性能获得可信性价值和客户满意度；
o） 合并保证计划，用于维持系统运行中的可信性性能。

6.2.3.2 可信性目标的要求

组织应针对相关职能、层次和可信性管理体系所需的过程建立产品可信性目标，应：
a） 具有可量化、可测试、可追溯、可维护等特点，能明确指导系统的设计、开发、运行、维护、改进等阶段；
b） 在系统的全生命周期内进行管理和控制，建立完善的可信性管理体系，确保系统满足可信性目标；
c） 基于系统的风险分析和评估，确定系统的安全完整性等级(SIL)和可信性等级(TRL)，并制定相应的验证和评估方法；
d） 符合国家法律法规、国家/行业/团体标准和技术规范的要求，体现城市轨道交通系统的安全性、可靠性、可持续性、经济性等特征。

6.2.4 可信性目标实现的策划

组织在建立可信性目标时，应：
a） 明确相关产品的可信性要求；
b） 进行可信性目标的分配和分析；
c） 确定可信性管理框架的结构形式；
d） 明确可信性各部门之间的职责权限；
e） 确定部门之间的关系及协调方法；
f） 确定需要的可信性资源；
g） 识别可能面对的风险和失效；
h） 进行可信性目标的验证；
i） 对可信性目标的实现进行监控和改进。

6.2.5 可信性大纲的策划

6.2.5.1 可信性大纲的建立

组织应建立、实施和保持成文的产品可信性大纲，每年对可信性大纲进行评审。组织在建立可信性大纲应考虑组织的技术和管理过程以及它们的限制和影响因素，包括：
a） 客户要求；
b） 法规要求；
c） 安全性要求；
d） 交付目标；
e） 允许的预算；
f） 可用资源；
g） 技术能力；
h） 环境影响；
i） 技术的新颖性；

j） 技术改进或迭代；
k） 提供可持续的服务。

6.2.5.2 可信性大纲的裁剪

在裁剪可信性大纲时，应考虑：
a） 辨别组织背景，包括方针和基础架构；
b） 考虑法规或标准的要求；
c） 辨别产品相关的特性，如特征和功能、相似产品的历史、特定的最终用途以及预期的应用环境；
d） 目标和要求分析；
e） 确定适用的特定寿命周期阶段或时期；
f） 评估风险和失效；
g） 选择关于已辨别的特定寿命周期阶段或时期的可信性活动；
h） 选择实现可信性所需的工具和技术活动；
i） 选择量度和评估技术；
j） 规定所需的能力和资源以及实际中可用的工具；
k） 资源的优先级和分配；
l） 策划评审和保证；
m） 形成关于裁剪原则的文档，并作为组织或项目计划一部分。

注：裁剪活动的结果构成了可信性计划的基础。

6.2.5.3 可信性计划

组织的产品可信性计划应作为基本的管理、策划和控制文件，支撑可信性大纲的执行。可信性计划的编制应与其他计划的编制一起综合考虑，并在开始一个新的工程项目或策划一个新的或改型的产品前进行正式的评审。

产品可信性计划应涉及影响产品可信性的所有活动，并清楚地规定为实现该计划管理者所承担的责任。应提出适合于工作项目的实施和控制的途径和方法，并保证实施的有效性。

可信性计划应包括：
a） 为该项目所选择的可信性项目/要素的确认和描述；
b） 为确保计划的项目得到恰当的实施，并与其他活动进行适当的协调所需的审核和评审项目的确认和描述；
c） 管理、实施和检查项目人员的职、责、权及相互关系的确认和描述；
d） 完成任务的程序细节，如时间进度、节点，以及设计评审、验证和确认准则的描述；
e） 为及时完成大纲中所确认的各项项目所需的资源的规定；
f） 在每个节点应交付的产品或文件的规定，以及负责开发、选取和使用所需文件的机构的确认；
g） 文件控制和技术状态管理体系的规定；
h） 为确保有关数据的协调传输，在可信性与有关学科之间建立信息联系；
i） 分包方控制。

6.2.5.4 可信性大纲的其他要求

在产品生命周期的所有阶段，组织应对可信性大纲：
a） 进行连续的定性和定量研究；
b） 可信性评估应不断更新，规定的要求应进行验证；
c） 各个要素应与开发、生产和运行大纲的其他要素形成统一整体。

6.3 变更的策划

6.3.1 组织应符合 GB/T 19001-2016 中 6.3 的要求。

6.3.2 当出现以下情形时，组织也应考虑策划变更可信性管理体系：

a) 可信性要求发生变化；

b) 由其他组织实施的可信性活动的对接情况发生变化。

7 支持

7.1 资源

7.1.1 总则

组织应符合GB/T 19001-2016中7.1.1和ISO 22163:2023中7.1.1.1的要求。

7.1.2 人员

组织应符合GB/T 19001-2016中7.1.2的要求。

7.1.3 基础设施

组织应符合GB/T 19001-2016中7.1.3的要求。

7.1.4 过程运行环境

组织应符合GB/T 19001-2016中7.1.4的要求。

7.1.5 测量溯源

组织应符合GB/T 19001-2016中7.1.5.1、7.1.5.2和ISO 22163:2023中7.1.5.3的要求。

7.1.6 组织的知识

组织应符合GB/T 19001-2016中7.1.6和ISO 22163:2023中7.1.6.1的要求。

7.1.7 组织的能力

组织为实现可信性目标还需要具备的资源和能力，包括但不限于：

a) 明确产品可信性负责人，主要负责可信性或可能作为另一个角色的一部分；

b) 进行适当的技术活动和分析的专业知识的人员；

c) 信息管理系统，如可信性知识数据库（独立或作为后勤保障系统的一部分）；

d) 适宜的可信性分析软件。

7.1.8 可信性信息管理系统

组织宜建立可信性信息管理系统，以实现对来自于各种可信性数据源数据的收集，特别是在生产中使用的产品或有系统参与的信息。可信性信息管理系统的建立，包括但不限于：

a) 与现有的信息管理系统框架、实施和使用方法兼容；

b) 对管理查询、访问和检索的及时响应；

c) 确保文档和报告的结构层次符合已建立的质量保证程序；

d) 能够填充足够的当前可信性数据和历史记录，以支持内部项目及协助服务运营过程中的产品部署；

e) 失效分析报告：故障信息闭环管理系统(FRACAS，或称失效报告、分析和纠正措施系统)(通常指硬件)失效记录，针对项目基本的可信性应用建立组织的程序和数据库；

f) 维修和后勤保障系统：支持系统服务操作；

g） 失效管理系统：获取系统错误和失效，尤其是与网络及软件相关的系统错误和故障，以便进行失效预防、缓解计划的实现和容错性的替代设计开发；
h） 可信性评估方法和技术：在系统可信性预测、分析和评估方面获取性能优化设计特性；
i） 信息保留：检索和传播可信性相关的记录和数据；
j） 知识的获取和捕捉：促进可信性知识开发。

7.2 能力

7.2.1 组织应符合 GB/T 19001-2016 中 7.2 和 ISO 22163:2023 中 7.2.1 的要求。
7.2.2 组织还应：
a） 确保有关组织成员都适当接受可信性相关内容培训，在整个培训过程中理解可信性管理体系内涵，并在规定的时间间隔进行有关可信性管理知识和岗位技能的考核；
b） 具备辨别失效行为的能力；
c） 具备对可信性管理范围内相关工作的管理与协调能力。

7.3 意识

7.3.1 组织应符合 GB/T 19001-2016 中 7.3 的要求。
7.3.2 组织应确保在其控制下的工作人员还应知晓：
a） 可信性管理的概念、目的、原则和方法以及组织的可信性文化；
b） 可信性管理体系的建立、实施、维护和改进的要求；
c） 可信性管理体系的文件控制、记录控制、内部审核、管理评审和持续改进的程序；
d） 可信性管理体系的变更管理、风险管理、问题管理和教育培训的规范；
e） 可信性管理体系的内外部沟通、协调和合作的方式；
f） 可信性管理体系的绩效评价、考核和激励的机制；
g） 岗位的可信性职责；
h） 有关可信性管理体系的文件化信息及其更改。

7.4 沟通

7.4.1 组织应符合 GB/T 19001-2016 中 7.4 和 ISO 22163:2023 中 7.4.1 的要求。
7.4.2 组织应确定与可信性管理相关的沟通需求：
a） 确保所有员工都了解可信性管理的原则和目标；
b） 定期向员工更新可信性管理的进展和成果；
c） 鼓励员工在可信性方面提出问题，并提供必要的支持和培训；
d） 在内部沟通中强调对可信性问题的重视，并鼓励员工在遇到问题时及时报告。

7.5 文件化信息

7.5.1 组织应符合 GB/T 19001-2016 中 7.5.1~7.5.3 和 ISO 22163:2023 中 7.5.3.3 的要求。
7.5.2 组织应对可信性管理过程中所涉及到的文件化信息进行管理，包括除本文件要求外的文件化信息，以及确保可信性管理体系有效性的文件化信息。该过程宜包含以下内容：
a） 创建可信性信息管理系统并对过程中涉及的信息进行存档，该系统应具有以下的功能：
1）识别各信息的特征；
2）对可信性信息进行分类；
3）信息的更新迭代。
b） 定期考核和评定信息系统的有效性；
c） 制定必要的规章制度和有关要求；

d） 实施信息的闭环管理；
e） 对信息管理人员进行技术培训；
f） 信息知识产权的保护。

8 运行

8.1 运行的策划和控制

组织应符合GB/T 19001-2016中8.1和ISO 22163:2023中8.1.1的要求。

8.1.1 投标管理

组织应符合ISO 22163:2023中8.1.2的要求。

8.1.2 项目管理

组织应符合ISO 22163:2023中8.1.3的要求。

8.1.3 配置管理和变更控制

组织应符合ISO 22163:2023中8.1.4的要求。

8.1.4 外包管理

组织应制定详细的供应商外包评价和管理机制，以确保其遵循的相应的可信性管理机制与本可信性管理体系一致。

组织在确定可信性管理体系的外包或过程转移管理时，应：

a） 遵循一定的流程和步骤，确保外包或转移的合理性、有效性和一致性；
b） 考虑相关方的需求和期望，及时通知并征求他们的意见和反馈；
c） 考虑外包或转移的可行性、必要性和紧迫性；
d） 考虑外包或转移的计划、实施、验证和确认；
e） 确定外包或转移的目的、范围、影响和风险；
f） 进行外包或转移的沟通、协调和控制；
g） 进行外包或转移的记录、审查和评估。

8.2 产品和服务的要求

8.2.1 顾客沟通

8.2.1.1 组织应符合 GB/T 19001-2016 中 8.2.1 和 ISO 22163:2023 中 8.2.1.1 的要求。

8.2.1.2 组织应与顾客沟通：

a） 产品和服务的功能和非功能要求以及可信性要求；
b） 顾客开展活动中的可信性管理要求；
c） 适用时，包括顾客与组织的外部供方就产品和服务可信性达成的共识。

8.2.1.3 与顾客沟通产品要求，还包括但不限于：

a） 约束条件（如安全性、环境、可持续性、退役、报废等）；
b） 使用环境；
c） 维修保障方针；
d） 试验或运行时发现的设计缺陷；
e） 验证和确认方法；
f） 验收程序以及可能的试验；
g） 维修保障程序；

h） 运行时产品性能状态的数据。

8.2.1.4 与顾客沟通服务要求，还包括但不限于：

a） 确定有效的程序收集顾客对服务的要求；

b） 建立便捷、有效的顾客反馈意见和投诉的渠道。

8.2.2 产品和服务要求的确定

8.2.2.1 组织应符合 GB/T 19001-2016 中 8.2.2 和 ISO 22163:2023 中 8.2.2.1 的要求。

8.2.2.2 组织应在产品和服务成本因素基础上，确定产品和服务生命周期内的可信性要求，并与功能要求和非功能要求协调。

8.2.2.3 对产品可信性要求的确定，组织应从以下方面考虑系统/产品可信性要求，包括但不限于：

a） 运行环境条件下的设计特性，如电磁兼容；

b） 应用条件下的设计特性，如人机界面；

c） 可维修的设计特性；

d） 首次失效时间或损坏时间；

e） 期望的产品总寿命；

f） 要求的维修性；

g） 退役；

h） 交付时限；

i） 成本限制等。

8.2.2.4 对运营服务可信性要求的确定，包括：

a） 组织应明确满足乘客需求的运营服务可信性要求，运营服务可信性要求通常与服务提供和服务保障的安全性、准时性、可靠性、便捷性、舒适性有关，可能包括但不限于：

— 期望的不中断运行时长；

— 行车与站厅的安全性；

— 站车环境设施和服务设施正常运行时长；

— 引导系统信息获取和更新的便利性和及时性；

— 维修和维修保障需求的能力和可用性等。

b） 组织应规定与运营服务可信性有关的设备设施的可信性要求，可能包括但不限于：

— 运行期间最大的允许失效率；

— 产品可用性和有效性的最小期望等。

8.2.3 产品和服务要求的评审

8.2.3.1 组织应符合 GB/T 19001-2016 中 8.2.3 和 ISO 22163:2023 中 8.2.3.1 的要求。

8.2.3.2 组织应确保有能力满足产品和服务的可信性要求，并应评审：

a） 产品和服务运行的使用条件和环境条件；

b） 产品和服务可信性的评判准则；

c） 产品和服务预定的功能；

d） 定义产品和服务失效及其判据；

e） 与顾客和第三方（如供应商）之间的责任；

f） 验证和确认方法；

g） 操作、维护、服务人员的要求；

h） 产品可信性与运营服务可信性的相关性；

i） 部署和使用产品及服务的方法；

j） 用于分析的可接受数据资源（如运行数据）等。

8.2.4 产品和服务要求的更改

组织应符合GB/T 19001-2016中8.2.4的要求。

8.2.5 产品和服务要求的补充

组织应符合ISO 22163:2023中8.2.5的要求。

8.3 产品的设计和开发

8.3.1 总则

8.3.1.1 组织应符合 GB/T 19001-2016 中 8.3.1 和 ISO 22163:2023 中 8.3.1.1 的要求。

8.3.1.2 设计和开发阶段的目的是计划和执行选取的工程设计方案，以实现产品的预定功能。组织对产品的设计活动应包括：

a) 架构设计；
b) 功能设计和评价；
c) 功能设计和评价包含以下过程：
   1) 建立功能设计准则；
   2) 可信性设计方法；
   3) 可信性设计策略；
   4) 系统应用环境设计；
   5) 人机交互设计；
   6) 设计功能的评价。

8.3.1.3 系统设计文档应包含以下可信性信息和数据：

a) 可信性工程项目计划：提供关于项目任务和支付时间表的关键信息，以支撑系统设计；
b) 可信性保证计划：提供保证策略和有计划的可信性工程活动；
c) 配置管理系统：系统结构基线，以及组成硬件和软件系统功能配置的持续更新；
d) 系统可靠性分配：分配给系统功能相关的可靠性数据；
e) 系统可信性评估：提供分析和评价数据如FTA、FMECA、失效分析等；
f) 系统设计可信性规范：提供相关的可信性特性，以进行定量评估和测量，验证系统设计的可信性要求是否得到满足；
g) 功能设计可信性规范：提供相关的可信性特性，以进行定量评估和测量，验证功能设计的可信性要求是否得到满足；
h) 功能测试规范：提供用于系统性能验证的功能测试规程；
i) 系统测试规范：提供用于系统性能验证的集成测试规程；
j) 失效报告、分析和纠正措施系统。

8.3.1.4 系统设计需要项目计划来启动特定子系统的开发，开发过程需要对资本和资源投资做出重大承诺，商业决策需要确定：

a) 关于项目开发条款和条件的合同协议；
b) 资本和资源投资的商业计划及实施战略；
c) 关于工作说明和目标交付时间表的项目计划；
d) 为支持项目开发而进行的招聘和培训资源规划；
e) 产品开发成果的可制造性和测试性；
f) 具备生产和制造能力；
g) 建立测试验证设施；
h) 建立配置管理规程；
i) 建立维修保障和后勤计划；

j） 建立失效分析的规程；
k） 制定客户联络和供应商合作协议；
l） 建立供应链管理规程；
m） 建立外包和分包规程；
n） 建立质量保证规程。

设计和开发还应完成维修保障计划、维修性、操作规程、保证和保障、技术迭代等过程计划的制定。

8.3.2 设计和开发策划

组织应符合GB/T 19001-2016中8.3.2和ISO 22163:2023中8.3.2.1的要求。

8.3.2.1 可信性预计

组织应在设计和开发阶段初期进行产品可信性预计，并随着设计工作的进展和数据的变动修正预计，其结果提供给管理者和设计者，并成为产品是否可行和保障条款是否符合可信性要求的反馈数据。

在设计早期，可信性预计可能是验证可信性要求的唯一方法。可信性预计也应用于各种权衡研究。可信性预计模型的建立应包括以下两步：

a） 结构模型：即建立表示部件状态或工作之间关系的逻辑模型；
b） 数学模型：即推导出代表结构模型的数学模型和公式，然后将逻辑模型各要素的数据输入数学模型并通过计算以获得结果。

注： 应通过可信性分析和预计在设计/开发的初期确认可信性关键部件。

8.3.2.2 权衡分析

设计权衡允许在各个生命周期阶段对要求的可信性水平进行选择。组织应在概念和定义阶段以及设计和开发阶段的早期进行权衡分析，权衡研究为可信性要求的分配提供输入。以后各阶段的权衡研究可使分配更精确，并有助于在各种设计和保障方案中进行选择。

组织进行的权衡分析应包括：

a） 可用性与维修性之间的权衡；
b） 维修性与维修保障之间的权衡；
c） 可靠性与产品性能之间的权衡；
d） 不同设计方案的可信性性能与生命周期费用的权衡。

8.3.2.3 产品可信性规定

组织应在设计和开发阶段的初期对产品的可信性进行规定，包括：

a） 识别正在考虑的系统：系统识别包括名称、预期的用途、使用或运行条件等；
b） 说明系统在主要应用方面的目的：描述要实现的系统性能目标或分配的要完成的任务；
c） 确定实现系统性能所需的关键功能：应从系统要求的角度说明每个功能的目的；
d） 描述完成系统任务运行所需的每个已识别的功能：提供关于功能的范围和目标；
e） 确定每项功能的影响因素：以评估其对系统的影响；
f） 评价实现功能的技术方法；
g） 描述功能中涉及的系统要素：确定实现要求功能的实用方法、合理的成本和效益手段；
h） 从可信性角度确定系统运行场景；
i） 系统架构设计应清晰描述与项目运行剖面场景相关的系统架构；
j） 通过建立系统运行场景，并结合评估过程中所确定的特定功能要求，来明确建立关于系统功能的可信性要求。

组织应保留相关的文件化信息。

8.3.3 设计和开发输入

组织应符合GB/T 19001-2016中8.3.3和ISO 22163:2023中8.3.3.1的要求。

8.3.3.1 可靠性设计

组织应在设计和开发阶段进行产品的可靠性设计，应包括但不限于：

a) 应用容错技术(冗余、并行编程、结构重组、重新启动)和失效-安全技术；
b) 应用自上而下设计、模块化编程、元器件降额设计等设计方法；
c) 消除致命的单点故障模式；
d) 控制作用于部件和元器件的应力；
e) 控制对软件有破坏作用的负荷；
f) 减少参数变化(如老化)对设计性能的影响；
g) 使用优选的和经过证实的部件和技术；
h) 规定降低制造和装配工艺敏感性的方法；
i) 符合安全准则；
j) 掌握部件的寿命演变规律或建立寿命预测模型；
k) 保证软件无故障的特殊技术，例如代码检验，代码审核和初查过程。

8.3.3.2 维修性设计

组织应在设计与开发阶段进行产品的维修性设计,应包括根据产品特定维修性要求编制出详细的维修性设计准则，并定期评审，以保证产品在服役过程中易于维护和修理。

产品维修设计应基于失效分析流程或失效分析报告进行。产品维修性要求设计应使下列各项减到最低限度：

a) 维修复杂度；
b) 产品设计规定的预防性维修活动的频率；
c) 产品的特殊性引起的不可用时间；
d) 产品设计规定的维修保障成本；
e) 对维修人员技术水平的要求；
f) 潜在的维修错误。

当设计工作是以现有的产品为基础时，该产品的维修性应该用文件描述清楚，任何已知的问题在开发阶段应予以考虑。

注：产品维修性设计应符合GB/T 9414.2-2012的要求。

8.3.3.3 维修保障性设计

组织应提出关于产品维修保障的要求，以保证产品的可靠性、安全性和经济性。主要内容应包括：

a) 维修保障性目标：产品在规定的使用条件和寿命期内，应达到的维修保障性水平；
b) 维修保障性设计：在产品设计阶段，根据维修保障性目标和原则，采用相应的技术和方法，使产品具有良好的维修保障性特性；
c) 维修保障资源：为实施产品的维修保障而需要的各种物质和人力资源；
d) 维修保障组织：为实施产品的维修保障而建立的各种管理机构和工作流程；
e) 维修保障评估：对产品的维修保障性进行定量或定性的分析和评价，以验证产品是否满足维修保障性目标，以及提出改进措施和建议。

注：维修保障评估应采用相应的技术和方法，如失效分析、FMECA、RCMA、可用度分析等。

组织应对产品的维修保障性进行设计，应包括：

a） 维修方针、方法、工具、测试设备、测试文件；
b） 保障方针所需的其他设施；
c） 维修人员的培训大纲等。

产品维修保障性设计应包括以下各项的确认和准备：
a） 与失效/故障和维修报告有关的数据收集、分析、评价的步骤和所需的资源；
b） 失效分析的结果及维修技术解决方案；
c） 对产品进行更改和改进的技术方案、步骤和所需的资源；
d） 确定由供方负责保障产品的期限。

当设计工作以现有产品为基础时，应对该产品的维修保障条件进行评审，对已知的问题予以考虑。

注：产品维修保障性设计应符合GB/T 9414.9-2017中第4章的要求。

8.3.3.4 测试性设计

组织应进行产品测试性设计，以保证产品的可靠性和维修性接受故障监控、探测，以及定位的内、外部设备对产品性能退化的影响进行实时反馈。例如使用失效/故障诊断与健康管理系统（PHM）监控系统。

可信性规范中阐述测试性要求（测试功能和步骤，产品每一级别的测试精度等）的部分应对这些设计工作提供指导。当设计工作以现有产品为基础时，该产品的测试性应该用文件描述清楚，已知的问题在开发阶段应予以考虑。

用于测试性的监控、探测设备应定期进行计量校准。

注：测试性要求应符合GB/T 9414.5-2018中的要求。

8.3.3.5 人因工程

设计活动应考虑人的因素，即人与产品本身的接口关系。产品设计工作的目的是在制造、安装、运行和维修、改进、处置等各生命周期阶段使人为错误及其影响减至最小。组织应通过人因工程确保：
a） 可信性不会因产品与操作和维修人员的相互作用而降低；
b） 操作和维修人员的培训与使用能经济有效；
c） 所有说明资料适用于预期的用户。

为确保满足产品的总目标，必要时，人因工程也应影响验证确认和试验活动的策划与执行。

8.3.4 设计和开发控制

组织应符合GB/T 19001-2016中8.3.4和ISO 22163:2023中8.3.4.1的要求。

8.3.4.1 设计评审

组织应符合ISO 22163:2023中8.3.4.2的要求。

组织应在重要的节点进行正式设计评审，其目的是为了确保正在开发的产品能满足可信性要求。应在所有生命周期阶段进行设计评审，评审应是对产品及其保障条件进行的正式的、独立的和客观的评价。

注：正式设计评审不只限于可信性评价这一目的。

设计评审应包括：
a） 最近的可信性预计；
b） 已确认的潜在的设计或保障的薄弱环节；
c） 失效模式和影响，失效树，应力和载荷，人因和权衡分析；
d） 以前评审工作的情况；
e） 验证和试验结果。

在以下各阶段应进行设计评审，并形成文件化件化信息：

a） 初步设计评审；

b） 详细设计评审；

c） 最终设计评审；

d） 制造设计评审；

e） 安装设计评审；

f） 使用设计评审。

供方可根据顾客的要求或指令，让顾客参与供方的设计评审工作。顾客应就供方的设计分析所要求的关于运行和维修保障条件的信息，与供方进行联系。

8.3.4.2 设计验证

组织应符合ISO 22163:2023中8.3.4.3~8.3.4.5的要求。

组织应建立和保持检验产品可信性要求是否满足的验证、确认和试验活动条件的程序。

试验活动应与正在设计的产品的功能试验日程安排(如单元试验综合试验和系统试验等)相适应。

注1: 试验应包括在摸拟失效/故障条件下进行的可靠性试验和维修性试验。

注2: 维修性试验应包括与正在试验的产品有关的手动和自动维修活动。

注3: 在产品有更改或变化时为确定产品的改进是否对可信性有非预期的不良影响应重复进行过去做过的试验。

应根据可信性规范和其他输入和规范，以及产品工程指南来编写验证、确认和试验方案，包括方法步骤和判据。

验证、确认和试验活动应与产品特性和可信性要求相适应。

注4: 通常根据产品的分级要求，从元器件到装配完好的系统都应逐级进行试验。应对每一级别分析可信性试验的可行性。

注5: 通常应在所有级别考虑可靠性试验而维修性试验只在某些级别进行。应在（实际或模拟的)现场条件下进行维修保障和可用性试验。

试验方案应规定试验项目、试验条件和试验方法，以及失效分析报告、分析的类型和应用的统计评价技术。

8.3.4.3 RAMS 管理的验证

组织应在产品的生命周期中对产品的RAMS管理进行验证，主要的验证任务应包括：

a） 用分析和测试方法验证制造管理产生RAMS审批的子系统和部件；

b） 用分析和测试的方法验证已安装的系统是否满足RAMS要求；

c） 评审信息的充分性、相应的数据和此阶段RAMS任务的输入；

d） 审批子系统和部件的实现以保证和RAMS验收标准包括周期要求相一致；

e） 指定的子系统、部件和外设总的组成结构应保证与整个系统RAMS要求相一致；

f） 子系统、部件和外设的RAMS要求应该在功能上保证完整一致；

g） 验证今后的所有周期工作计划和系统RAMS要求相一致，包括周期费用要求；

h） 评审验收计划和审批计划的充分性和完整性；

i） 修订后的安全规划和审批计划应该保证能长期应用；

j） 评审操作数据采集系统的有效性和充分性；

k） 各阶段内从事这些任务的全体职工的能力的评审；

l） 评审在本阶段内方法、工具和技术充分性。

8.3.4.4 寿命试验

组织应在设计和开发阶段或制造阶段中进行寿命试验，以探测和确认产品的薄弱环节，确定产品的耐久性并为纠正措施以及维修保障策划等提供信息。

注：寿命试验属于失效分析流程中的部分，可以单独开展，也可以结合模拟、仿真或其他分析。

8.3.4.5 可靠性增长试验

组织应对产品可靠性增长试验进行统计与评估，统计试验与评估方法应符合GB/T 39844-2021中所规定的要求。

8.3.5 设计和开发输出

8.3.5.1 组织应符合 GB/T 19001-2016 中 8.3.5 和 ISO 22163:2023 中 8.3.5.1 的要求。

组织应根据产品的结构和维修安排，对可信性要求进行验证和确认，以及设计进展过程把可信性要求分配给产品的各部件。

8.3.5.2 最终产品的任何分包部件的规范中，都应包含可信性要求的分配，并用作验证、确认和试验程序的规定和设计的基础。

8.3.5.2 组织应确保设计过程输出的过程，包含：

a) 满足可信性要求的子系统和部件的方案；
b) 满足可信性要求的子系统和部件的施工设计；
c) 在可信性管理范围内为今后的寿命周期工作建立计划，包括：
   1) 安装计划；
   2) 调试计划；
   3) 运营和维修计划；
   4) 运营中数据获取和评估。
d) 定义、验证和建立能够生产已确认的符合可信性要求的子系统和部件的制造工序，可用措施包括：
   1) 环境应力筛选；
   2) RAM 改进测试；
   3) 对 RAMS 有关失效模式进行检查、测试和分析。

8.3.6 设计和开发更改

8.3.6.1 组织应符合 GB/T 19001-2016 中 8.3.6 的要求。

8.3.6.2 组织应对产品和服务在设计和开发期间，以及后续所做的更改进行适当的识别、评审和控制。组织应：

a) 确保对设计和开发阶段所做的更改符合顾客可信性要求；
b) 对更改过后会产生的影响进行评估；
c) 建立改进策略和计划；
d) 保证组织内部成员与相关方知晓更改过程；
e) 保留设计开发更改相关文件化信息。

8.4 外部提供的过程、产品和服务的控制

8.4.1 总则

8.4.1.1 组织应符合 GB/T 19001-2016 中 8.4.1 和 ISO 22163:2023 中 8.4.1.1 的要求。

8.4.1.2 组织应对外部提供的过程、产品和服务实施控制，包括：

a) 确定外部提供的过程、产品和服务的可信性要求；
b) 确定供应链的可行性以及协作的风险；

c） 对外部提供的过程、产品和服务进行风险评估；
d） 对过程、产品和服务进行风险评估；
e） 保留外部提供的相关文件化信息。

8.4.2 控制类型和程度

8.4.2.1 组织应符合 GB/T 19001-2016 中 8.4.2 和 ISO 22163:2023 中 8.4.2.1~8.4.2.3 的要求。
8.4.2.2 当产品的部件由二级供(分包方)提供时，一级供方应确保：
a） 部件符合相关产品规范要求；
b） 相关部件应符合适应部件属性的可信性特性（包括但不限于可靠性、可用性、维修性和保障性等）的定性与定量要求；
c） 这些部件的要求充分满足整个交付产品的要求。
8.4.2.3 当供应商提供要交付的产品或部件时，供方应要求顾客提供：
a） 部件按照符合可信性大纲进行设计和制造的证据；
b） 对最终产品进行可信性分析和评价所需的有关数据和信息；
c） 部件可能遇到的问题。

8.4.3 提供给外部供方的信息

8.4.3.1 组织应符合 GB/T 19001-2016 中 8.4.3 和 ISO 22163:2023 中 8.4.3.1 的要求。
8.4.3.2 提供给外部供方的信息还应包括但不限于：
a） 产品和服务预定的功能；
b） 产品和服务运行条件；
c） 维修方针；
d） 维修性规范；
e） 维修服务响应要求；
f） 维修说明书；
g） 验证和确认方法等。

8.4.4 供应链管理

组织应符合ISO 22163:2023中8.4.4的要求。

8.5 生产和服务提供

8.5.1 生产和服务提供的控制

组织应符合GB/T 19001-2016中8.5.1和ISO 22163:2023中8.5.1.1的要求。

8.5.1.1 生产调度

组织应符合ISO 22163:2023中8.5.1.2的要求。

8.5.1.2 特殊进程

组织应符合ISO 22163:2023中8.5.1.3的要求。

8.5.1.3 生产设备

组织应符合ISO 22163:2023中8.5.1.2的要求。

8.5.1.4 产品可信性控制

组织应在生产提供过程中对产品可信性进行控制，受控条件包括但不限于：

a） 产品可信性大纲、质量保证大纲；
b） 外部供方可信性大纲；
c） 测试和诊断大纲；
d） 集成计划；
e） 失效报告、分析、数据收集和反馈系统；
f） 产品监控、诊断方案、事件报告和数据管理系统；
g） 验证和确认计划；
h） 安装计划。

8.5.1.5 服务可信性控制

组织应对服务可信性进行控制，受控条件包括但不限于：

a） 服务组件的服务配置管理，该过程应定义服务组件及其配置项，并对配置项的变更予以控制；
b） 服务提供过程的确认，包括：
— 识别、确定服务提供过程的每一个服务组件及其配置项；
— 识别、确定服务提供过程的每一个服务组件及其配置项的功能或能力要求；
— 服务提供过程预演结果的认定，包括服务保障和服务失效恢复；
— 变更后的再确认。

8.5.2 标识和可追溯性

8.5.2.1 组织应符合 GB/T 19001-2016 中 8.5.2 和 ISO 22163:2023 中 8.5.2.1 的要求。

8.5.2.2 组织应提供有效的方法来确保可追溯性，包括监控可信性活动的进程并能追溯到其初始要求的必要措施。

8.5.3 顾客或外部供方的财产

组织应符合GB/T 19001-2016中8.5.3和 ISO 22163:2023中8.5.3.1的要求。

8.5.4 防护

8.5.4.1 组织应符合 GB/T 19001-2016 中 8.5.4 和 ISO 22163:2023 中 8.5.4.1 的要求。

8.5.4.2 组织应在生产和服务提供期间对输出进行必要的防护，以确保符合要求，包括：

a） 建立产品安全性、安保和可靠性设计准则；
b） 在产品规格说明书中合并可信性要求；
c） 对符合可信性要求的产品张贴质量安全标签。

8.5.5 交付后活动

8.5.5.1 组织应符合 GB/T 19001-2016 中 8.5.5 和 ISO 22163:2023 中 8.5.5.1 的要求。

8.5.5.2 组织应满足与产品和服务相关的交付后活动的要求。组织应为交付后活动建立、实施和保持文件化过程。此过程应包括：

a） 交付后各方职责归属文件；
b） 为安全相关操作提供的警告标签和程序；
c） 提供的产品保修信息；
d） 提供的产品质量认证声明；
e） 提供可靠性和可用性报告；
f） 产品可靠性和维修性信息，性能历史和保障测试数据验证清单；
g） 产品质量信息和质量记录验证清单；

h） 产品符合性评估数据验证清单；
i） 产品维修记录验证清单。

8.5.6 更改控制

8.5.6.1 组织应符合 GB/T 19001-2016 中 8.5.6 的要求。
8.5.6.2 组织应建立和保持控制产品更改的正式程序，它包括对更改要求的说明、更改后果的评价、更改的批准和授权、更改的实施和验证职费的规定。
8.5.6.3 组织应建立、维持和定期评审可信性更改大纲。
8.5.6.4 组织应对产品或其服务的任何改进实施与原来产品及其服务相同的可信性验证。
8.5.6.5 组织应确保技术状态管理系统支持更改过程。

8.6 产品和服务的放行

8.6.1 组织应符合 GB/T 19001-2016 中 8.6 和 ISO 22163:2023 中 8.6.1 的要求。
8.6.2 组织应严格把握对可信性产品和服务的放行要求，确保：
a） 对产品和服务的放行得到有关授权人员的批准；
b） 产品和服务的放行不会影响产品质量；
c） 放行后的产品符合客户的可信性要求；
d） 不会损害相关方的利益；
e） 保留放行过程相关文件化信息。

8.7 不合格输出的控制

8.7.1 组织应符合 GB/T 19001-2016 中 8.7.1、8.7.2 和 ISO 22163:2023 中 8.7.3 的要求。
8.7.2 组织应对不满足可信性要求的输出进行识别与控制，以防止其非预期的使用和交付，组织应：
a） 按照可信性要求对产品质量进行评估；
b） 分析对可信性管理的潜在有害影响；
c） 对不合格的产品进行纠正与改进；
d） 保留不合格产品输出的文件化信息。

8.8 运营和维修的控制

8.8.1 运营目标

组织应对产品的运营目标进行确定，包括：
a） 确保达到服务水平；
b） 满足客户对产品可信性的期望；
c） 监控安全性（例如应用PHM系统），确保系统安全性满足期望；
d） 监测产品可靠性增长，确保达到可靠性目标；
e） 为运营成本分析和可信性价值评估收集信息；
f） 最小化不可用时间，促进产品的可用性，提高工业制造的产能；
g） 关注外部环境因素，确保符合法律法规，以及社会等的特殊使用要求；
h） 重视失效分析对持续改进的贡献；
i） 识别运行服务改进的机会。

8.8.2 运营和维修的可信性工程活动

8.8.2.1 组织应对产品在运营和维修期间所涉及的可信性活动进行计划与确定，包括：
a） 实施现场数据收集或计算机化的维修管理；

b） 开展用户满意度调查；
c） 开展问题的失效分析；
d） 评审/更新维修大纲；
e） 推荐用于持续改进的技术方案或程序变更；
f） 确定服务质量。

8.8.2.2 组织应保留有关运营和维修可信性工程活动的文件化信息。

8.8.3 维修性大纲

8.8.3.1 组织的维修性大纲应包含以下要素：
a） 确保有效执行维修性大纲的管理和组织活动；
b） 在设计阶段开展一系列维修性分析工作；
c） 失效分析的方案。

8.8.3.2 维修性大纲的编制应考虑以下方面的因素：
a） 用户适用性；
b） 与产品有关的因素：
1） 维修性要求：为提供规定的可用性而要求的维修性和维修保障水平；
2） 复杂度：产品的复杂度将决定维修保障设备的复杂度；
3） 大纲限制：应考虑附加的维修活动来满足产品的可信性要求；
4） 维修保障条件：维修方针和维修人员的技术水平都会使维修工作的有效性受到影响；
5） 用户相关的因素：用户的维修经验、用户执行维修活动的程度、产品对用户的重要性；
6） 供应商相关因素：供应商的维修经验和供应商所能提供的维修保障的程度将决定可能采取的维修活动的场所和维修等级；
7） 失效分析：应通过失效分析提供维修技术和方案的改进；
8） 生命周期阶段：即使产品不需要制定完整的研制大纲，但仍需与满足产品要求的维修分析一起考虑相关的产品寿命周期阶段要求。
c） 产品可用性与LCC之间的权衡；
d） 维修和维修保障需求与LCC之间的权衡；
e） 安全隐患的消除。

8.8.3.3 组织应详细说明影响产品有效使用的失效/故障类型，并通过分析确定以下内容：
a） 维修性定量要求：系统的维修性规范、维修性演示验证和维修性保证要求，是维修性定量要求的一部分，系统或分系统的维修性通常是用平均有效维修时间（MAMT）来定量，同时给出了一个最大维修时间，还可包括进一步详细的要求；
b） 维修性定性要求：包括产品功能的定义、失效/故障判据、环境条件和使用条件，以及满足要求的有效使用寿命；
c） 测试性要求：包括测试功能和程序、产品各级别测试准确度、测试设备的要求等。

注：组织对产品进行维修性分析应符合GB/T 9414.1的要求。

8.8.4 失效数据采集

组织应收集关于产品失效分析和统计分析所需的数据。包括但不限于：
a） 可靠性：应包括发生的失效和有关故障影响的信息；
b） 可用性：应包括与每一故障（指对在可信性规范中规定的可用性度量有影响的故障）有关的不能工作时间；

c） 维修性：应包括对每一次失效测量维修性所需的信息，其中包括预防性维修中故障未发现时间和修复时间（必要时应包括这些时间的各个组成部分），也应记录所有必需的修理实施时间的各个组成部分；
d） 维修保障性：应包括与可信性规范中说明的维修保障性能度量有关的管理延误和后勤延误；
e） 维修费用。

注：组织对产品维修性相应数据的收集、分析与表示应符合GB/T 9414.3的要求。

8.9 首件检验

8.9.1 组织应符合 ISO 22163:2023 中 8.9 的要求。
8.9.2 组织应在产品首件检验过程中对产品的可信性要求进行检验，检测的内容包括：
a） 检验产品是否符合客户可信性要求规范；
b） 检验产品全生命周期可信性文件是否齐全；
c） 对不符合可信性要求的产品采取纠正措施；
d） 保留对首件产品可信性要求检验的文件化信息。

8.10 老化管理

组织应符合 ISO 22163:2023 中 8.10 的要求。

8.11 创新管理

组织宜建立、实施和保持一个成文文件化过程，以管理新产品、服务和技术的创新，此过程宜包括：
a） 识别和监测其经营环境中的变化；
b） 制定创新规划；
c） 确定创新项目的优先次序；
d） 考虑利益相关方的参与。

9 绩效评价

9.1 监视、测量、分析和评价

组织应符合 GB/T 19001-2016 中 9.1 和 ISO 22163:2023 中 9.1.1.1、9.1.2.1、9.1.3.1 的要求。

9.2 内部审核

9.2.1 组织应符合 GB/T 19001-2016 中 9.2.1、9.2.2 和 ISO 22163:2023 中 9.2.3.1、9.2.3.2 的要求。
9.2.2 组织应按照策划的时间间隔进行内部审核，以提供有关可信性管理体系的下列信息：
a） 可信性管理体系的符合性：即是否符合组织的可信性方针、目标、程序和其他文件，以及适用的法律法规和其他要求；
b） 可信性管理体系的有效性：即是否能够实现组织的可信性目标和预期结果，包括可靠性、安全性、可用性、可维护性和可测试件等指标；
c） 可信性管理体系的改进机会：即是否能够识别和应对可能影响可信性管理体系符合性和有效性的风险和机遇，以及采取纠正措施和持续改进措施。

9.3 管理评审

9.3.1 组织应符合 GB/T 19001-2016 中 9.3.1~9.3.3 和 ISO 22163:2023 中 9.3.1.1、9.3.2.1、9.3.3.1 的要求。

9.3.2 组织对于可信性管理的评审，还应包括：

a) 可使用概率评估和建模方法进行预测；
b) 产品提供方可通过可靠性加速和寿命试验等方法进行估计；
c) 服务提供方可利用统计和其他方法进行量度和分析；
d) 确保通过制定政策指导和实施流程的行动方案来实现组织业务目标；
e) 定期确定组织、子公司部门、制造工厂或服务设施的健康和运行状况；
f) 确保项目计划的活动按预定时间完成，满足约定的项目需求；
g) 确保系统和产品设计的实现和评估与设计需求是一致的；
h) 确保系统性能和保障服务能够充分维持持续的运营并为顾客提供服务。

9.3.3 过程评审

组织应符合 ISO 22163:2023 中 9.4 的要求。

10 改进

10.1 总则

10.1.1 组织应符合 GB/T 19001-2016 中 10.1 的要求。

10.1.2 组织应建立和保持一个能系统地确定和执行产品可靠性、维修性以及维修保障性能的任何必需改进的程序。这种可信性改进大纲应采用以适当的统计和失效分析技术分析的有关数据为基础，特别是应阐明产品的可信性关键部件。

10.1.3 组织应在整个设计和开发阶段建立和保持实时有效的失效分析程序和分析报告，并扩展到制造阶段/安装阶段，以及继续扩展到运行和维修阶段。

10.2 不符合和纠正措施

组织应符合 GB/T 19001-2016 中 10.2 和 ISO 22163:2023 中 10.2.3 的要求。

10.3 持续改进

10.3.1 组织应符合 GB/T 19001-2016 中 10.3 的要求。

10.3.2 组织应注重可信性管理的持续改进，根据产品和服务的运行反馈和客户需求，不断优化可信性管理流程和方法，提高可信性管理效率和效果，提升产品和服务的安全性、可靠性和可用性等。

10.3.3 组织应建立、实现和定期检查控制系统修改和更新的程序，包括：

a) 建立一个反馈循环系统，通过失效分析和技术方案，确保实际与运行情况和新的技术发展不断的更新完善；
b) 对于所有的修改和更新任务的相应周期模式的强制使用的控制；
c) 在修改和更新之后要求建立一个验证、审批和验收系统RAMS性能的程序；
d) 分析变动的原因；
e) 做一个变动的RAMS影响分析，包括周期费用要求的影响；
f) 计划执行和随即的验收变动；
g) 记录修改和更新任务；
h) 更新所有受影响的系统文件。

组织应考虑对可信性管理体系分析与评价的结果以及管理评审的输出，以确定是否需要对可信性管理体系进行修改，这些输出将作为可信性管理体系持续修改的参考。

10.3.4 组织在可信性管理体系的运营过程中，应当定期分析和评价体系的运行状况，并根据评价结果和管理评审的输出，对体系进行必要的调整和改进。

10.4 持续改进阶段可信性活动

组织应对持续改进阶段的可信性工程活动形文件化过程，主要活动包括：

a) 评价由新增变化引起大的可信性影响；
b) 评价所采取的变更对生命周期费用的影响；
c) 开展风险和价值评估；
d) 开展变更后的用户满意度调查；
e) 管理软件版本的发布。

10.5 失效分析和技术解决方案

10.5.1 失效分析报告和流程

组织应建立失效分析流程和失效/故障报告的制度，应明确：

a) 失效分析流程是城市轨道交通产品的持续改进阶段的必要管理流程，组织应设置相关主管部门负责失效分析，失效分析工作可由该部门负责或采用服务外包来实施；
b) 失效报告是在城市轨道交通运营过程中，因设备、系统、人员等原因造成运营安全和服务质量受到影响的事件的报告；
c) 失效报告应包括发生单位、时间、地点、现场情况、初步原因分析、已采取的措施、下一步计划等内容，并应在事件发生后1小时内向上级主管部门报告；
d) 失效分析主管部门在接到失效报告后，及时启动应急措施和失效分析流程。

组织应针对产品的特性制定失效分析的流程，并对其实施过程进行控制。

组织应建立、实施和保持文件化过程以管理产品失效分析报告和技术解决方案，包括：

a) 对服役后的失效产品与部件进行及时的失效分析，形成失效分析报告和技术解决方案；
b) 评审失效产品及部件对运营过程中的影响；
c) 建立闭环失效/故障报告系统；
d) 评审失效产品/部件技术解决方案。

为满足运行和保障条件而进行设计变化和更改时应重新考虑失效分析的有效性。如有可能失效分析的结果可用于定性可信性要求的验证和确认。

失效分析应能够：

a) 确认影响可信性的关键产品部件或保障活动；
b) 确认需要连续注意及表明维修方针有必要更改的有限寿命部件。

10.5.2 技术解决方案

组织开展的失效分析除了进行事故/故障责任判定外，还要获得产品失效的原因和机理，并给出改进、预防或减缓失效后果的技术解决方案。包括且不限于：

a) 系统结构设计改进或局部参数的优化；
b) 材料匹配的改进或新材料的引入，或材料制造工艺、组织结构、性能的调控与优化；
c) 表面处理的采用或优化，包括表面处理的技术方法、工艺参数、材料体系选择、加工方案等；
d) 制造工艺优化或装配工艺优化；
e) 产品的修程或修制的优化或改变；
f) 资源配置或管理流程的优化；
g) 产品延寿技术的采用，实现寿命周期的延长；
h) 针对报废零部件，采用产品再制造技术，实现零部件再次进入生产、应用循环；

i） 质量管理体系改进。

技术方案的有效需要经受LCC分析的评价。

10.5.3 失效整改的措施和监督

失效分析报告和技术解决方案应通过验证和组织的内外部评审后，才可用于失效整改。

失效整改是指根据失效分析报告提出的技术解决方案所制定的改进措施，应确定：

a） 制定整改方案和时限，消除隐患，防止再次发生类似事件；

b） 失效整改应由运营单位负责实施，并由主管部门进行监督检查，确保整改措施有效落实。