ICS 25.040
N 10

中华人民共和国国家标准

GB/T 34071—2017

物联网总体技术
智能传感器可靠性设计方法与评审

General technology for internet of things—
Reliability design method and review for intelligent sensor

广东省网络空间安全协会受控资料

2017-07-31 发布　　2018-02-01 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

广东省网络空间安全协会受控资料

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本标准起草单位：上海工业自动化仪表研究院、北京瑞普三元仪表有限公司、天信仪表集团有限公司、绵阳市维博电子有限责任公司、西安东风机电有限公司、北京国电智深控制技术有限公司。

本标准主要起草人：谢亚莲、李振中、李孝评、阮赐元、张鹏、麻贵峰。

广东省网络空间安全协会受控资料

物联网总体技术
智能传感器可靠性设计方法与评审

1 范围

本标准规定了物联网总体技术中智能传感器在研制过程中的可靠性设计以及对可靠性设计进行评审的方法和要求。

本标准适用于物联网总体技术中智能传感器在硬件方案论证阶段、技术设计阶段、详细设计阶段、试生产(生产定型)阶段的可靠性设计工作和评审工作,以及在产品需求分析阶段、软件需求分析阶段、软件概要设计阶段、软件详细设计阶段和软件实现阶段的可靠性设计工作和评审工作。各企业可以根据产品的特点和研制需要,适当增减内容。

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 2900.13 可靠性、维修性的基本术语和定义

GB/T 34068 物联网总体技术 智能传感器接口规范

3 术语和定义

GB/T 2900.13 界定的以及下列术语和定义适用于本文件。

3.1

物联网 internet of things

基于互联网、传统电信网等信息载体,让所有能够被独立寻址的普通物理对象实现互联互通的网络。普通对象设备化、自治终端互联化和普适服务智能化是其三个重要特征。

3.2

物联网智能传感器 intelligent sensor in internet of things

位于物联网的感知识别层的信息生成设备,将被测量转换为物联网可传送的标准化输出信号的传感器。

3.3

可靠性设计评审 reliability design reviews

对现有的或建议的设计所作的正式的和独立的检查,用以找出可能影响可靠性、可维修性的设计薄弱环节以及提出可能的改进措施,以加速设计成熟的一种审核。

3.4

可靠性工作项目 reliability work item

仪表研制过程中完成的可靠性设计报告、性能与功能测试报告、环境试验报告、可靠性增长试验报告、可靠性鉴定试验报告和现场试运行报告的总称。

广东省网络空间安全协会会员资料

3.5

平均修复时间　mean time to repair;MTTR

产品从发现故障到恢复规定功能所需要的时间的平均值(即故障检测、故障定位、故障诊断、故障维修时间之和的平均值)。

3.6

平均故障间隔时间　mean time between failure;MTBF

可修复产品的一种可靠性参数,是故障间隔时间的平均值。

4　可靠性设计方法

4.1　概述

物联网智能传感器(以下简称产品)由硬件和软件构成,完整的物联网可靠性设计包括硬件可靠性设计、软件可靠性设计和通迅的可靠性设计。

4.2　硬件可靠性设计

4.2.1　可靠性设计要求

4.2.1.1　产品在研制任务书中应明确规定可靠性的定性或定量要求。

4.2.1.2　可靠性设计的定性要求包括成熟设计、简化设计、模块化设计、抗环境干扰设计、EMC 设计、测试性和维护性设计等。

4.2.1.3　产品可靠性的定量要求包括可靠度 $R(t)$、失效率 λ、平均故障间隔时间 MTBF、可用度 A。

4.2.1.4　可靠性设计是产品设计的一部分,应与产品设计同时进行。

4.2.2　可靠性各阶段设计要求

4.2.2.1　方案论证阶段

4.2.2.1.1　方案设计阶段的可靠性设计要求包括:

a)　应明确产品的可靠性设计指标要求值,如 $R(t)$、MTBF、MTTR、λ、A 等。

b)　应明确在产品设计中采用的可靠性技术措施,包括可靠性建模、预计和分配,热设计,EMC 设计,安全性设计,测试性、维修性设计,故障模式影响分析(FMEA),元器件和电路的容差分析等。可以根据产品的实际需求选择其中的几种。

c)　应明确产品使用环境,说明产品的工作温度、电磁干扰、防潮、防震、贮存及运输等环境条件的要求。

d)　制订产品研制计划、试验计划和费用分析等。

4.2.2.1.2　方案设计阶段形成的文件资料包括:

a)　产品总体设计技术方案;

b)　产品可靠性设计可行性分析报告。

4.2.2.2　技术设计阶段

4.2.2.2.1　技术设计阶段的可靠性设计要求包括:

a)　建立可靠性数学模型;

b)　完成产品的可靠性分配,将产品的可靠性指标值逐层分解;

c)　初步完成产品的可靠性预计,可采用元器件计数法或相似设备法;

d)　完成关键件的失效判据、失效模式和效应分析,确立薄弱环节。

广东省网络空间安全协会受控资料

4.2.2.2.2 技术设计阶段应提交的技术文件资料包括：

a) 可靠性分配方案；

b) 初步可靠性预计报告；

c) 关键件可靠性分析报告。

4.2.2.3 详细设计阶段

4.2.2.3.1 详细设计阶段的可靠性设计要求包括：

a) 在产品的可靠性设计中可采用简化设计、模块化设计、冗余设计、热设计、环境防护设计、抗冲击、振动设计等；

b) 电路的可靠性设计中可采用简化方案，避免片面追求高性能指标和过多的功能，合理划分软硬件功能和合理的元器件使用；亦可综合热设计、容差与漂移设计、电气互连的可靠性设计、电磁兼容设计、故障诊断设计等；

c) 元器件级的可靠性设计应关注器件的选择与使用，可采用降额设计、器件面向使用电应力设计和失效机理分析；

d) 应完成产品的可靠性预计；

e) 应完成产品的失效模式、影响和危害度分析。

4.2.2.3.2 详细设计阶段的应提交的技术文件资料包括：

a) 产品设计说明；

b) 产品可靠性预计报告；

c) 产品失效模式、影响和危害度分析报告。

4.2.2.4 试生产阶段

4.2.2.4.1 试生产阶段的可靠性设计要求包括：

a) 应编制关键件明细表，规定重点控制元器件、零部件；

b) 对选用的原材料、元器件、外协件的质量控制；

c) 解决影响产品可靠性所有薄弱环节；

d) 批试的产品应经过各种环境试验、可靠性试验和工业现场使用的评定。

4.2.2.4.2 试生产阶段的应提交的技术文件资料包括：

a) 试生产暴露的问题和解决的措施；

b) 环境试验、可靠性试验的试验记录和试验报告；

c) 工业用户现场使用工作报告、失效分析和失效记录；

d) 使用和维护说明书。

4.3 软件可靠性设计

4.3.1 软件可靠性设计要求

4.3.1.1 产品在研制任务书中应明确规定软件可靠性设计的定性要求，若有软件可靠性指标，应规定软件可靠性指标的要求。

4.3.1.2 软件可靠性设计的定性要求包括执行软件需求分析、软件危险分析。

4.3.1.3 软件可靠性设计的定性要求包括可靠性设计方法，如结构设计、模块化设计、冗余设计、接口设计、健壮设计、简化设计、余量设计、防错程序设计、编程要求、更改要求。

4.3.1.4 若有软件可靠性指标，应确定软件可靠性模型和软件可靠性的评估方法。

广东省网络空间安全协会受控资料

4.3.2 软件可靠性各阶段设计要求

4.3.2.1 产品需求分析阶段

4.3.2.1.1 产品需求分析阶段的可靠性设计要求包括：

a) 对具有高可靠性和安全性要求的功能，应分析用硬件实现还是软件实现的利弊，作出决策；

b) 分配的软件可靠性指标应与硬件的可靠性指标大体相当；

c) 应自动记录产品故障；

d) 应规定防止越权或意外地存取或修改软件的保密性设计；

e) 对可靠性要求高的功能应考虑软件的容错设计。

4.3.2.1.2 产品需求分析阶段应提交的技术文件资料包括：产品需求分析。

4.3.2.2 软件需求分析阶段

4.3.2.2.1 软件需求分析阶段的可靠性设计要求包括：

a) 软件需求规格说明应无歧义性、完整性、可验证性、一致性、可修改性、可追踪性；

b) 对关键软件，应列出可能的不期望事件，分析导致这些不期望事件的可能原因，提出相应的软件处理要求；

c) 对有可靠性指标的软件，在确定了软件的功能性需求之后，应考虑软件的可靠性指标是否能够达到以及是否能够验证，还应与用户密切配合，确定软件使用的功能剖面，并制订软件可靠性测试计划；

d) 对安全关键软件，在软件开发的各个阶段进行有关的软件危险分析；

e) 应规定接口设计，包括硬件接口的软件设计、人机界面设计、报警设计、软件接口设计；

f) 应规定在哪个方面进行软件健壮性设计，如电源失效防护、加电检测、电磁干扰、错误操作等；

g) 应考虑资源分配和时序安排的余量设计；

h) 应规定数据要求。

4.3.2.2.2 软件需求分析阶段应提交的技术文件资料包括：软件需求分析报告。

4.3.2.3 软件概要设计阶段

4.3.2.3.1 软件概要设计阶段的可靠性设计要求包括：

a) 对安全关键软件，应进行软件危险分析；

b) 对安全关键软件的设计应遵循规定的原则；

c) 若需冗余设计，概要设计冗余；

d) 概要设计接口设计；

e) 概要设计软件健壮性设计；

f) 设计模块的简化设计；

g) 实现余量设计；

h) 实现数据要求；

i) 在软件设计中应实现防错程序设计；

j) 应规定并执行软件更改的要求。

4.3.2.3.2 软件概要设计阶段应提交的技术文件资料包括：

a) 软件概要设计说明书；

b) 软件危险分析；

c) 软件更改影响分析报告(若存在软件更改)。

广东省网络空间安全协会受控资料

4.3.2.4 软件详细设计阶段

4.3.2.4.1 软件详细设计阶段的可靠性设计要求包括：

a) 对安全关键软件，应进行软件危险分析；

b) 对安全关键软件应遵循规定的原则进行详细设计；

c) 进行详细的冗余设计；

d) 进行详细的接口设计；

e) 进行详细的软件健壮性设计；

f) 模块的简化设计原则进行详细的模块设计；

g) 在软件详细设计中应满足数据要求；

h) 在软件详细设计中应实现防错程序设计；

i) 在软件详细设计中应满足编程要求；

j) 在软件详细设计中应满足多余物的处理的要求；

k) 应执行软件更改的要求。

4.3.2.4.2 软件详细设计阶段应提交的技术文件资料包括：

a) 软件详细设计说明书；

b) 软件危险分析；

c) 软件更改影响分析报告(若存在软件更改)。

4.3.2.5 软件实现阶段

4.3.2.5.1 软件实现阶段的可靠性设计要求包括：

a) 应进行软件的检查和测试，采取自检、互检和专检的软件检查，并按规定的要求进行软件测试；

b) 若存在软件可靠性指标，应确定软件可靠性模型，执行软件可靠性评估和预计程序。

4.3.2.5.2 软件实现阶段应提交的技术文件资料包括：

a) 软件测试计划和测试报告；

b) 软件可靠性评估报告。

4.4 数据通信的设计要求

智能传感器产品的数据通信的设计应按照 GB/T 34068 的要求进行。

应估算通信过程中的失效量(例如残余错误率)，包括传输错误、重复、删除、插入、重新排序、误用、延时和伪装。在估算由于随机硬件失效时应该考虑上述的失效量。

数据通信应提交的技术文件资料包括：

a) 接口数据通信设计详细说明书；

b) 数据通信概率测试计划；

c) 数据通信概率测试报告。

5 可靠性评审

5.1 可靠性设计评审概念

智能传感器产品在设计的各阶段，尤其是在设计决策的关键时刻，组织非直接参加设计的各有关方面专家，对设计进行及时的、详细的论证过程。

产品省网络空间安全协会受控资料

5.2 可靠性设计评审的作用

进行设计质量控制，在设计阶段及时发现和纠正潜在的设计缺陷实现智能传感器的可靠性。

5.3 评审目标

设计评审的主要目标是通过对设计依据、设计方法和设计结果的分析、审查，从而揭露可靠性和维修性设计上的不足和薄弱环节，以便为设计改进提示方向。

设计评审的具体目标是：

a) 检查可靠性设计的正确性；

b) 提出产品设计中存在的薄弱环节；

c) 提出改进可靠性、可维修性的建议；

d) 评审智能传感器结构工艺，降低成本的可能性。

5.4 评审组织机构

成立评审组。评审组人员及职责参见附录 A。

5.5 评审内容及要求

5.5.1 硬件可靠性设计评审

5.5.1.1 设置评审点

可分别选择方案论证阶段、技术设计阶段、详细设计阶段、试生产(生产定型)阶段参照表 1 设置评审点、选择评审项目。

广东省网络空间安全协会受控资料

表 1 设计阶段与设计评审类型的示例

设计阶段	工作	评审类型	评审时机示例
方案论证阶段	确定产品的可靠性指标要求，采取的可靠性设计措施，及产品的使用环境	设计输入评审	a) 收到设计合同或授权后。 b) 方案论证完成后
技术设计阶段	建立产品的可靠性模型，完成产品的可靠性分配，初步完成产品的可靠性预计以及关键件的失效分析	方案设计评审	a) 在完成方案设计后。 b) 为了给计划和成本评估提供足够详细的信息时
详细设计阶段	在产品的设计中采用可靠性设计措施，完成可靠性预计，以及失效模式、影响和后果分析	详细设计评审	a) 在完成详细设计后。 b) 通过原型试验来验证设计
生产定型阶段	应编制关键件明细表，规定重点控制元器件、零部件；对选用的元器件、外协件的质量控制；批试产品经过各种环境试验、可靠性试验和现场使用已证明符合规定要求	生产定型设计评审	完成整个产品设计后
注：在不同的节点进行的设计评审要设定不同的名称，如“方案论证评审”和“详细设计评审”。这些名称对于不同的组织机构是不相同的。在表中给出的名称只是举例并非权威性的，在使用时按实际设计项目来确定名称。			

5.5.1.2 设计评审内容

可靠性评审按产品硬件设计的各阶段进行。各阶段的评审内容和所提交的技术文件资料见 4.2.2。

5.5.2 软件可靠性设计评审

5.5.2.1 设置评审点

可分别选择产品需求分析阶段、软件需求分析阶段、软件概要设计阶段、软件详细设计阶段、软件实现阶段参照表 1 设置评审点、选择评审项目。对数据通信的评审可放在软件可靠性设计评审中。

5.5.2.2 设计评审内容

可靠性评审按产品软件设计的各阶段进行。各阶段的评审内容和所提交的技术文件资料见 4.3.2。

5.6 设计评审程序

5.6.1 制定设计评审计划

应明确哪个或哪几个节点要开展设计评审在设计计划阶段。开展设计评审可以避免作出费钱、费时的难以挽回的决定。这样，任何由设计评审引起的变化对进度或成本造成的影响都会较小一些。如果在设计过程中的重要节点上进行评审，成本、进度和性能改进都会更容易被接受。

在设计评审进程中设计主管应考虑具体项目要求的条件和限制，并应确定最佳评审次数，以从花费的时间中得到最大的回报。

召开预审会议，确定设计阶段和评审类型的设置，制定评审进度和各设计阶段的评审项目，重点应放在新的设计特性、新采用的材料和元器件、新的计算和试验方法上。完成各设计阶段评审项目清单(见表 2)，设计评审项目检查清单中每一项的具体问题参见附录 B。明确评审组成员分工。

广东省网络空间安全协会受控资料

表 2 设计评审清单

序号	评审项目	评审阶段			
		方案论证	技术设计	详细设计	定型
1	设计合同、技术协议书或技术任务书	☆			
2	产品设计要求和产品使用环境分析	☆			
3	可行性分析： (1) 指标的合理性； (2) 实现的可能性		☆		
4	产品功能图、可靠性框图、可靠性分配		☆		
5	初样的设计准则		☆		
6	拟采用的新技术、新工艺、新材料及解决情况		√		
7	安全性和维修性设计		√		
8	质量保证大纲及其工作计划			√	☆
9	可靠性预计			☆	
10	关键零部件的失效模式、效应分析			☆	
11	产品的失效模式、效应分析或故障树分析			☆	

表 2（续）

序号	评审项目	评审阶段			
		方案论证	技术设计	详细设计	定型
12	关键元器件降额和冗余设计的评定			☆	
13	对寿命有限的部件检查和更换方针			☆	
14	当可靠性预计结果低于目标值时，拟采取的措施			☆	
15	可靠性验证试验或可靠性增长试验计划				
16	环境适应性设计			☆	
17	对可靠性验证试验或可靠性增长试验中已出现的失效分析及防止失效再可靠性验证试验或可靠性增长试验发生的措施			☆	
18	元器件、零部件、原材料的优选，标准化、系列化、通用化的评定			√	☆
19	影响产品质量的关键工艺			√	☆
20	机械和电子部件的连接			√	☆
21	工业用户现场使用试验： (1) 试验方案； (2) 失效记录； (3) 统计计算方法			☆	☆
22	定型产品规范、试验规范、验收规范和使用维护规范			☆	
23	质量管理： (1) 管理机构和人员的配备； (2) 制造过程中的质量保证要求； (3) 外协件的质量控制和监督				☆
注：☆表示该评审阶段必须完成的审查项目；√表示可以根据具体情况选取审查项目，由评审小组决定。					

广东省网络空间安全协会受控资料

5.6.2 选择设计评审人员

5.6.2.1 概要

设计评审通常由一个独立的评审组来执行，该组从负责设计的人员那里获得信息。设计评审人员通常包括：

a) 设计评审组。包括：
- 组长；
- 秘书；
- 能说明白那些会影响产品或过程质量和性能的，但又不直接参与设计的人；
- 不参与受审产品开发的相关专家；
- 有实际经验的消费者/用户。

b) 设计主管和设计组成员。设计评审组应包括不同领域的有专业知识和经验的人，其成员应能覆盖涉及产品各方面足够宽和足够细的知识领域。应注意将评审组的规模控制在一个可运转的范围内。

5.6.3 准备评审材料

设计主管负责汇总与即将进行的设计评审有关的信息。根据评审计划，负责研制的主要设计人员，

填写阶段设计评审计划表(参见附录C)报组织实施部门,并将本阶段评审所需的资料汇总整理后,在评审会议之前,应考虑一个提前期,送交评审小组成员,以便他们充分掌握内容。

根据不同的设计阶段,评审材料应包括以下全部或部分内容:

a) 设计计划(包括技术协议书或技术任务书);

b) 原始要求(可包括用户提出对报价、规范、标准和管理要求);

c) 关于设计设想的文档;

d) 对设计的权衡研究和分析(包括方案论证和技术先进性分析);

e) 设计评审组对受审设计的提问清单;

f) 可靠性、可用性以及维修性分配、预计和失效模式及效应分析;

g) 后勤保障计划(包括关键原材料、元器件、外协质量控制和质量保证以及产品质量保证大纲);

h) 设计者的建议和可选事项,包括图纸和计算;

i) 类似产品的信息和数据;

j) 竞争产品的数据;

k) 成本估计及其权衡原则;

l) 技术规范和图纸;

m) 制造、加工和可生产性研究;

n) 性能要求、测试报告及其分析;

o) 现场失效和故障报告;

p) 供货和工艺质量控制分析;

q) 检验报告;

r) 寿命周期目标和费用数据。

5.6.4 会议通知和议程

秘书应协助组长准备会议通知和议程(包括要讨论的主题),并发送给参会者,使参会者在设计评审前做好充分的准备。在通知和议程中应说明:

a) 会议日期、时间和地点;

b) 设计评审的目的和范围;

c) 项目名称和编号;

d) 参加者及其职责;

e) 设计评审的类型和持续时间;

f) 如果合适的话,说明项目中受审的部分;

g) 要讨论的主题,如:

- 对设计项目目标的评审;
- 对产品设计特性和性能参数的描述;
- 对当前的设计和技术进展情况,以及遇到的问题的评审;
- 对尚未完成和以后的工作、以及所有相关事项的评审;
- 对照设计评审检查清单,对设计的各有关方面的全面评估;
- 由评审组所做决定的概要;

h) 发言人员名单;

i) 相关文件和所有附上的评审材料目录。

广东省网络空间安全协会受控资料

5.6.5 主持设计评审会议

5.6.5.1 概要

评审组长应审查会议的目标，并将其与设计评审过程的所有目标和程序联系起来，并应着重考虑提问的必要性，避免一些负面的，有个人倾向的意见。避免提出含有过早判断的问题。

评审组成员可自由地对与会代表提问，在任何时候，应确保所有提出的问题，要求的后续调查以及发表的看法都不会影响任何参加评审人员的人格、能力和威信。评审组应在组长领导下确保设计评审过程不会变成组员之间或与设计小组之间的个人争辩。

评审组的成员应牢记他们的顾问身份，他们的主要目的是协助产品设计达到最优效果，而不是为已确认的缺陷提供解决方法。

5.6.5.2 情况介绍

设计主管和其他代表设计和开发小组的成员应按要求介绍受审设计的有关情况。

5.6.5.3 会议草案

评审过程是一个建设性提问和回答的过程，应根据需要的信息或要了解某些设计和开发决定的理由来构成问题，也不允许断然拒绝讨论某项主题，除非有涉及商业机密或国家安全方面的内容。

评审组成员可预先将一些问题提交给组长，为了保证会议的进程，次要的问题可在会前先了结，其余问题将作为会议准备资料的一部分，以便允许相关人员作好回答的准备。

设计评审过程无权批准或不批准受审的设计开发文件。

5.6.5.4 实施项目

无论何时要采取措施，都应在会议纪要中记录指派人的姓名、交代的任务以及回应的日期。

因为评审组的身份是顾问，所以设计主管要对所有实施项目做出回应。

5.6.5.5 建议

如何要记录这些建议的理由。建议不同于实施项目，但在其后建议也可能成为实施项目。

5.6.5.6 未完成的实施项目和被拒绝的建议

对于那些来自早期设计评审且尚未完成的实施项目，以及被拒绝的建议，应解释并记录没有实施或拒绝的理由。

5.6.5.7 会议结束

在会议的结论中组长应总结由评审得出的措施和建议以确保评审组达成共识。

5.6.6 准备和分发设计评审会议记录

设计评审会议记录由评审组秘书处分发给参加会议的有关人员。

5.6.7 设计主管对措施与建议做出反馈

设计主管对会议中提出的措施与建设性建议应及时做出回应，进行合理改进，并将结果反馈给有关部门。

广东省网络空间安全协会受控资料

5.6.8 贯彻执行措施与建议

贯彻执行措施与建议都完成了，将记录交设计主管签署。

5.6.9 结束

设计主管签署记录，结束记录。

广东省网络空间安全协会受控资料

附 录 A
（资料性附录）
评审组成员职责

表 A.1 给出了在设计阶段评审组成员的职责。

表 A.1 评审组成员的职责

评审组成员的专业	职责	设计评审类型		
		方案设计	详细设计	定型设计
组长	召集、主持会议、发布中期报告和定型设计报告	×	×	×
秘书	收集、分发资料和文件，准备报告，协助组长	×	×	×
产品设计师	通过试验和计算的数据介绍设计和决策的理由	×	×	×
独立设计师	建设性地评审设计和结构是否完全满足客户需求	×	×	×
可靠性	评估和验证设计的可靠性已达到要求	×	×	×
维修性及维修	确保在设计中已考虑安装、维修和操作人员需要考虑的事项	×	×	×
质量	提供质量计划，确保检测、控制和试验能有效实施	×	×	×
计量测试	对计量器具和测试仪表选择的正确性和使用合理性进行审查			
后勤保障	提供综合后勤保障计划	×	×	×
环境影响	评估产品制造、使用和处理对环境产生的影响	×		
产品的安全性	关注有关规章、警告、数据收集、纠正措施和试验结论	×	×	×
人因	根据人的能力和局限性评估设计的方便实用性	×	×	×
合法性	评估设计是否与合同和法律条款相符，以及设计妥协和由产品使用和处理产生的问题的法律影响	×		×
制造	确保设计是可以按最低成本和进度生产的	×	×	×
生产工艺	对设计是否能经济合理地进行加工生产提出意见			
采购（供方、可选）	确保可获得满足费用和交付时间要求的有用的产品、部件和材料	×	×	
材料	确保挑选的材料能符合要求	×	×	
加工	根据要满足的容限和要求的功能所需的加工成本来评估设计	×	×	×
包装和运输	确保产品是能不受损地搬运和运输的			×
市场/销售	确保客户要求是符合实际并被所有人都充分理解的	×		×
客户（可选）	能对设计是否可接受表达意见，并能在某些细节问题上要求开展进一步研究	×		×
注：×表示该阶段应有该专业成员的意见。				

广东省网络空间安全协会受控资料

附 录 B
（资料性附录）
设计评审检查清单中的问题

B.1 概述

设计评审检查清单为确保提出应在设计评审会议上提出的要点提供了一种工具。在会议结束后，完成的检查清单为会议期间提出的事项及其建议和措施提供了一份记录。它可以作为会议记录的附件。检查清单不能替代评审组成员的知识和经验。

其设计要求，而这些问题完全取决于产品或过程的类型，对产品的性能特征不可能给出一种通用的清单。但有一些通用的设计问题（如下面给出的例子）是可以在设计评审中提出的。

每次设计评审，要推荐专人确定受审产品或过程需要讨论的特性。

B.2 可靠性

可靠性问题可包括：

a) 可靠性要求，例如，平均故障间隔时间（MTBF）、平均首次失效前时间（MTTFF）、失效率和期望寿命等，软件的可靠性指标与硬件的可靠性指标的符合性；
b) 在设计评审时，将产品或过程实际或预计的可靠性与相应的要求进行对比，包括假设、模型和数据来源；
c) 在项目计划中设定了令人满意的可靠性和成本目标；
d) 通过失效模式及影响分析（FMEA）和/或故障树分析（FTA）确定产品失效最有可能的原因，如最前的十种；
e) 提高可靠性的措施，如元器件的改进、替换、降额和环境控制，软件的多样性设计；
f) 要达到规定的可靠性需要用专门的生产工艺，包括环境步进应力试验、筛选和分析；
g) 对与产品可靠性相关的采购元器件的运输包装、运输以及存储要求；
h) 影响产品可靠性的运输包装、货运和储存条件；
i) 产品的储存寿命与要求的对比，包括假设、模型和数据来源；
j) 相似和竞争产品或过程的可靠性记录；
k) 安装、维修对可靠性的影响；
l) 用户对可靠性的影响；
m) 预定的可靠性测定和验证试验计划，如样品数、试验时间、试验条件和试验循环周期等。

广东省网络空间安全协会受控资料

B.3 维修

维修问题可包括：

a) 维修策略的评审涉及与规范和操作要求相关的维修梯队和维修等级；
b) 使用可更换单元应考虑：标识、互换能力、好处和风险、可达性、可移动性、运输包装和标识以及测试设备要求；
c) 采用嵌入式和插件程序以及通用试验设备来检测和诊断故障；
d) 提供无损伤检测。

B.4 维修性

维修性问题可包括：

a) 对于每个维修梯队和维修等级，维修性问题都包括平均修复时间(MTTR)和维修工时(NNH)的定量要求；

b) 维修性设计和预计要求的一致性，或维修性指标和分配与维修性观测值的比较；

c) 维修性设计分析，例如：在可靠性、维修性、维修保障性、可达性和诊断设备之间权衡；

d) 通过维修性验证试验对维修性进行验证；

e) 相似或竞争产品或过程的维修性记录。

B.5 维修保障

维修保障问题可包括：

a) 对于每个维修梯队和维修等级，维修性问题都包括平均修复时间(MTTR)和维修工时(MMH)的定量要求；

b) 维修性设计和预计与要求的一致性，或维修性指标和分配与维修性观测值的比较；

c) 维修性设计分析，例如：在可靠性、维修性、维修保障性、可达性和诊断设备之间权衡；

d) 通过维修性验证试验对维修性进行验证；

e) 相似或竞争产品或过程的维修性记录。

广东省网络空间安全协会受控资料

B.6 可用性

可用性问题可包括：

a) 用失效模式和影响分析(FMEA)和/或故障树分析(FTA)来确定产品被拒收的最有可能的原因，如最前面的十种；

b) 可用性要求，如平均可用度、瞬时可用度、使用寿命；

c) 产品或过程的预计可用度与要求的对比(包括假设、模型和数据来源)；

d) 改进可用度的措施，如模块比、引入冗余、元；

e) 器件替换、降额、环境控制、快速分离的应用；

f) 相似产品和竞争产品的性能；

g) 运行环境及现场保养对可用性的影响；

h) 运行和维修所用的专用设备和工具；

i) 用户因素对可用性的影响，如人员培训及其可用性、设备的误用、不合适的工具和元器件；

j) 预定的可用性测定和验证试验计划，如样品数、试验时间、试验条件和试验循环周期。

B.7 质量保证

质量保证问题可包括：

a) 与用户需求和满意度有关的事项；

b) 将材料、产品和过程的就是规范与用户需求进行对比；

c) 通过设计原型的测试来确认设计；

d) 在预期的使用和环境条件下工作的能力；

e) 无意识的使用和误用；
f) 遵守管理要求、国家和国际标准以及公司惯例；
g) 与各种竞争产品的设计进行对比；
h) 与相似设计的对比，尤其要分析内部和外部曾出现过的问题，以防再出现同样的问题；
i) 与产品规范和服务要求有关的事项；
j) 允许的公差和与加工能力的比较；
k) 接收/拒收准则；
l) 装配和安装的便利性、储存的要求、储存寿命和可处置性；
m) 良性失效和失效安全性；
n) 美学规范和接收准则；
o) 诊断和解决问题的能力；
p) 标签、警告、证明、可测性要求、用户指南和文件控制；
q) 标准件的评审和使用；
r) 与工艺规范有关的条款；
s) 设计的制造能力、包括特殊工艺要求、机械化、自动化、零部件的装配和安装；
t) 产品的检测和试验能力，包括特殊检测和试验要求；
u) 校准要求；
v) 材料、零部件和组件的规范，包括经认可的供应品和供应商及供应能力；
w) 运输包装、货运、储存和储存寿命等要求，特别是与进、出事项相关的安全因素；
x) 与设计验证有关的事项；
y) 备选的计算，用来验证原始计算和分析的正确性；
z) 开展试验，如通过模型或原型样机试验，确定试验程序并整理试验结果；
aa) 对原始计算和其他设计活动的正确性进行独立(第三方)验证；
bb) 构造上的控制，要有充分的识别功能；
cc) 生产日期和序列号、产品信息的评估和验证、位置记录及其参考点、标明的编码或未编码的信息。

B.8 环境对产品的影响

环境对产品的影响问题可包括：

a) 确定可能对产品或工程产生影响的环境条件，如温度、湿度、风和降水量等气候因素，放射物的影响，化学药品及其随时间发生的反应，尘埃、电磁辐射和射频干扰；
b) 确定是否已妥善考虑了环境对电子元器件、机械零部件、印制电路板、连接器、机械结构、磁介质等的影响；
c) 确定使用场地的预期条件是否符合规范；
d) 对比使用场地实际的环境条件与研发周期预期的条件；
e) 考虑是否应对给(确)定的使用场地的最重要环境参数(如温度、湿度)进行监控并付诸实施；
f) 操作人员在现场环境中安全工作的技巧；
g) 对外界动力源噪音、闪电的耐受程度，以及防止这些干扰的设施；
h) 污染物和水、雪、尘埃造成的影响；
i) 在维修中或元器件在加热中/冷却中掉电的情况下，超出产品的环境极限所产生的影响；
j) 考虑产品是否需要特殊的环境防护或环境适应性的鉴定试验；
k) 考虑以试验室模拟的方法来评估产品在不同环境条件下的性能；

广东省网络空间安全协会受控资料

l) 考虑与实际条件相关的试验准则；

m) 确定何时的环境试验加速因子。

B.9 产品的安全性

安全性问题可包括：

a) 确保产品中已适当地配有紧急断路开关、锁定控制、标记、标牌、断路器、防接地错误、烟雾传感器等装置；

b) 产品预期的用途、用户使用权限及其分类，包括年龄段、用户对潜在危险的意识及其身体条件的限制；

c) 环境条件，如温度范围、湿度、日照和雨水；

d) 管理所有使用场合设计安全性的法律、规定和标准；

e) 来自外部机构的安全认可；

f) 安全隐患，如化学性能(腐蚀性、毒性和易燃性)、爆炸、内爆、电击、着火、过热、辐射和机械特征(夹缝和锋利的边缘)；

g) 误用或滥用的危险；

h) 在生产或质量控制过程中意外的安全事故；

i) 对产品所做的安全试验的难度和受操作人员的错误操作影响程度；

j) 从制造到使用期间，产品安全性能的下降；

k) 可行且适当的警告和指示；

l) 对外购元器件潜在风险的评估、第三方试验和证明；

m) 自动保护装置的性能评估。

广东省网络空间安全协会受控资料

B.10 人因

人因问题可包括：

a) 提供给操作人员处理、控制和调整产品或过程的信息的自然状态和复杂性；

b) 操作人员用来控制产品或过程的信息输出(包括表达媒介)的有效性；

c) 与人的预期相关的产品特性，以及正常和紧急情况下做出的反应；

d) 对于操作、安装、维修、装配和处置，警告和指示是否合适和充分；

e) 评审在预期和预知的环境条件(维修、标识、工作空间)下，人与操作、维修和保障要求的接口；

f) 考虑在使用产品时操作人员的舒适度；

g) 为产品配备的器械是否放在显眼位置；

h) 产品控制的可达性；

i) 评估安装、操作和维修人员的技能和训练在产品或过程设计中被考虑的程度；

j) 详细评估显示要求(格式、数字、滚读显示)；

k) 产品软件程序和文件是否容易使用；

l) 对指示产品运行、状态和故障的听觉或视觉警告的需求及其类型；

m) 评审提高人因性能和简化人与产品互动难度的准则；

n) 产品操作和维修所需的所有文件及其说明的使用和理解是否适当、准确、明白和简易；

o) 操作人员技能已列入培训要求中；

p) 有权使用产品的非熟练操作者的潜在困难；

q) 由于操作者误用产品引起的潜在困难。

附 录 C
（资料性附录）
设计评审计划表

表 C.1 给出了设计评审计划阶段的设计评审计划表。

表 C.1 设计评审计划表

产品名称		规格型号	
产品类型		评审阶段	
参加设计人员		主管设计师	
本阶段目标及达到水平概述：			
本阶段设计方案及质量保证措施：			
提交审查的设计、试验资料清单：			
序号	名称	编写人	
上级主管部门审批意见：			

广东省网络空间安全协会受控资料

广东省网络空间安全协会受控资料

中 华 人 民 共 和 国
国 家 标 准
物联网总体技术
智能传感器可靠性设计方法与评审
GB/T 34071—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 38 千字
2017 年 8 月第一版 2017 年 8 月第一次印刷
*
书号:155066·1-56581 定价 24.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

GB/T 34071-2017