

QJ

中华人民共和国航天行业标准

FL 0110

QJ 1544B—2004
代替 QJ 1544A—1996

航天产品不合格、失效和危险分类

Nonconformity, failure and hazard classification for space products

2004 - 09 - 01 发布

2004 - 12 - 01 实施

国防科学技术工业委员会 发布

前 言

本标准代替QJ 1544A—1996《航天产品缺陷、不合格、故障和危险分类》。

本标准是航天产品保证系列标准的支撑标准之一，本修订版本针对航天产品的特点和发展要求，根据近年来对国内外产品保证技术的研究及工程应用经验总结，以航天产品不合格、失效和危险的分类为主要内容，为航天型号工程研制中质量、可靠性与安全性问题的分析与评价提供指导。修订后仍保持原标准的结构框架及内容安排，与前一版本相比，主要有以下变化：

- a) 修订后标准项目名称更改为《航天产品不合格、失效和危险分类》。
- b) 增加了按发生的原因进行不合格分类的内容。
- c) 根据缺陷的定义及“缺陷”应慎用的要求，删除对缺陷的分类要求和内容；如具体产品有缺陷分类要求时，可参照 GJB 179A—1996《计数抽样检查程序及表》（等效采用 MIL—STD—105E—1989）的相关内容进行分类。
- d) 根据故障和失效的定义并参照国内外相关标准，将“失效 failure”与“故障 fault”按两个术语分别定义。
- e) 主要针对“失效 failure”分类提出相关原则、方法和技术内容，替代原标准对“故障 failure , fault”进行分类的相关内容，以适应航天新型号研制工作和国际交流的需求；当具体产品有要求时，失效 failure 分类的要求和内容也适用于对故障 fault 的分类。
- f) 与 QJ 2731—1995《航天产品质量与可靠性信息分类与代码》相协调，对失效“按发生的原因分类”加以调整和细化，以适应航天新型号研制工作需求。
- g) 增加了按是否为系统性失效的分类（分为 A 类失效及 B 类失效），以适应航天型号研制中 FME (C) A 和可靠性试验等的实际需要。
- h) 参照 QJ 3026—1998《软件异常分类》（idt IEEE STD 1044—1993）、QJ 1317《电子元器件失效分类及代码》等标准，增加软件异常（失效）分类、电子元器件失效分类的相关要求和内容，以适应航天型号研制中软件和电子元器件可靠性工程的实际需要。
- i) 对危险严重性和危险可能性等级分类的要求和内容进行了必要的调整，以便与 QJ 2236A—1999《航天产品安全性保证要求》等标准协调一致。

本标准的附录A是资料性附录。

本标准由中国航天科技集团公司提出。

本标准由中国航天标准化研究所归口。

本标准起草单位：中国航天标准化研究所，中国航天科工集团第二事业部，中国航天科技集团一院、五院。

本标准主要起草人：伍平洋、周海京、王凤卿、朱美娴、谷 岩、肖名鑫。

本标准于1988年4月首次发布，1996年4月第一次修订，本次为第二次修订。

航天产品不合格、失效和危险分类

1 范围

本标准规定了航天产品不合格、失效和危险分类的要求和技术内容。

本标准适用于航天产品在研制、生产、试验和使用各阶段对不合格、失效和危险的分类及其信息的收集、分析、传递及利用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包含勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 3187—1994 可靠性、维修性术语

GJB 451 可靠性维修性术语

GJB 900—1990 系统安全性通用大纲

GJB/Z 9000A—2001 质量管理体系 基础和术语

QJ 1317 电子元器件失效分类及代码

QJ 3026—1998 软件异常分类（idt IEEE STD 1044—1993）

3 术语和定义

GB/T 3187—1994、GJB 451、GJB 900—1990、GJB/Z 9000A—2001确立的以及下列术语和定义适用于本标准。

3.1

缺陷 defect

未满足与预期或规定用途有关的要求。

注1：区分缺陷与不合格的概念是重要的，这是因为其中有法律内涵，特别是与产品责任问题有关。因此“缺陷”应慎用。

注2：顾客希望的预期用途可能受供方信息的内容的影响，如所提供的操作或维护说明。

[GJB/Z 9000A—2001的3.6.3]

3.2

不合格（不符合） nonconformity

未满足要求。

注：要求是明示的、通常隐含的或必须履行的需求或期望。

[GJB/Z 9000A—2001的3.6.2]

3.3

失效 failure

产品终止完成规定功能的能力这样的事件。

[GB/T 3187—1994的4.1.1]

3.4

故障 **fault**

产品不能执行规定功能的状态。预防性维修或其它计划性活动或缺乏外部资源的情况除外。故障通常是产品本身失效后的状态，但也可能在失效前就存在。

[GB/T 3187—1994的4.2.1]

3.5

危险 **hazard**

可能导致事故的状态。

[GJB 900—1990的3.3]

3.6

软件异常 **software anomalies**

与需求规格说明、设计文档、用户文档、标准等文档不一致的，或与人的感觉或经验不一致的任何情况。异常可能发现于软件产品或文档资料的评审、测试、分析、编译或使用期间，但也不局限于这些。

[QJ 3026—1998的3.1]

4 不合格分类

不合格是指通过检验、试验或其它方式，判定产品的质量特性（功能的或物理的）不符合合同、图纸、样件、技术条件或其它技术文件规定的要求。根据不合格的严重程度和其发生的原因进行分类。

4.1 按不合格的严重程度分类

4.1.1 严重不合格

与产品执行规定的功能相关的不合格为严重不合格，规定的功能如：

- a) 功能特性、使用特性；
- b) 功能接口或物理接口；
- c) 互换性；
- d) 形状、材料、质量、重心；
- e) 可靠性、维修性、安全性；
- f) 人员的健康与安全；
- g) 其它严重不合格。

4.1.2 一般不合格

严重不合格以外的其它不合格为一般不合格。

4.2 按不合格发生的原因分类

按不合格发生的不同原因进行分类，导致不合格的原因包括：

- a) 设计，如设计差错、设计不协调等；
- b) 工艺，如工艺不完善、工艺设计差错、工艺方法选择不当等；
- c) 操作，如不按工艺规程、试验规范、操作作业指导书操作等；
- d) 管理，如管理不当、制度不健全、不按规章工作等；
- e) 器材，如元器件、材料、外购件问题等；
- f) 软件，如软件未按工程化要求设计、未经评测等；
- g) 设备，如设备问题等；

- h) 环境，如环境因素影响等；
- i) 其它，上述原因以外的其它原因。

5 失效分类

根据失效判据及其它相关要求对失效进行分类。

5.1 按关联、非关联分类

为解释试验或工作结果或计算可靠性特征量值时，应对产品发生的所有失效按关联或非关联进行分类。

5.1.1 关联失效

在解释试验或工作结果或者计算可靠性特征量值时，应计入的失效都是关联失效。关联失效包括：

- a) 设计或工艺缺陷失效：由于产品设计缺陷或工艺缺陷造成的失效；
- b) 零、部件及元器件失效：由于零部件及元器件有缺陷造成的失效应计为关联失效。当数个同类型零、部件及元器件发生失效时，如果证明不是由某个失效引起另一个失效或几个失效，则每个失效应分别记为独立的关联失效；
- c) 耗损件失效：耗损件在寿命期内所发生的失效为关联失效；
- d) 多重失效：在同时发生多个零件失效，而且每个零件失效均能独立地阻碍设备正常工作的情况下，则每个失效应记为关联失效；
- e) 间隙失效：间隙失效是指产品发生失效后，不经修理而在有限时间内自行恢复功能的失效。间隙失效在第一次出现时应记为一个关联失效；
- f) 机内测试设备（BITE）失效：BITE 的每一次虚警，如果是独立的，应记为一个关联失效；
- g) 软件失效：与产品有关的计算机软件异常引起的失效，应记为关联失效；
- h) 其它关联失效：不属于上述 a) ~ g) 的其它关联失效。

5.1.2 非关联失效

在解释试验或工作结果或者计算可靠性特征量值时，不应计入的失效都是非关联失效。非关联失效包括：

- a) 使用和试验过程中，由于安装不当造成的失效；
- b) 试验设施、监测设备的失效以及由此而造成的失效；
- c) 由操作人员误操作造成的失效；
- d) 耗损件在寿命期限之后出现的失效；
- e) 从属失效：由于另一个产品的失效或故障而直接或间接引起的失效；
- f) 由于试验程序方面的错误而造成的失效；
- g) 在同一部位第二次及以后相继出现的间隙失效；
- h) 在筛选、寻找故障、修复验证或正常维护调整中发生的失效；
- i) 完全是由于超过设计要求的过应力所造成的失效；
- j) 批准的试验程序中明确规定的其它非关联失效。

5.1.3 关联失效变更为非关联失效

在研制或批生产中，为评定产品的可靠性，如果满足下列所有条件时，对已经划分为关联失效的，可以变更为非关联失效：

- a) 已按相应的可靠性试验规范或标准对提取可靠性试验样品的试制或生产批中的所有产品都采取了纠正措施；
- b) 所积累的试验数据已足以说明纠正措施对消除失效完全有效；
- c) 已得到顾客（订购方）对失效分类进行变更的批准。

5.2 按责任、非责任分类

为便于制定和实施有效的纠正措施，防止失效重复出现，可根据失效的原因是否属于产品研制或生产的某组织责任范围，将失效划分为责任失效与非责任失效。

5.2.1 责任失效

按合同（协议书）规定是该研制或生产组织责任范围内的原因造成的关联失效均属责任失效。

5.2.2 非责任失效

所有非关联失效或按合同（协议书）规定不是该研制或生产组织责任范围内的原因造成的关联失效均属非责任失效。

5.3 按系统性、偶然性分类

在进行FME（C）A和可靠性试验中，需要根据是由某一固有因素引起的还是由于偶然因素而随机出现的失效，而将失效划分为系统性失效和偶然（残余）性失效。

5.3.1 系统性失效

系统性失效是指肯定与某个原因有关的，只有通过修改设计或制造工艺、操作程序、文件或其他关联因素才能消除的失效。系统性失效可以通过对其产生原因的模拟来诱发。

5.3.2 偶然性失效

偶然性失效是由于偶然因素而随机出现的失效，这类失效通常难以重现。

5.4 按需要和不需要作纠正性更改分类

在进行FME（C）A和可靠性试验中，对系统性失效还可根据不作纠正性更改和需要作纠正性更改，分为A类失效和B类失效。

5.4.1 A类失效

由于费用、时间、技术上的限制或其它原因，由管理者决定不作纠正性更改的系统性失效。

5.4.2 B类失效

由管理者决定需作纠正性更改的系统性失效。

5.5 按失效的严重程度分类

5.5.1 类：灾难性失效（catastrophic failure）

导致导弹、运载火箭、卫星等系统丧失：系统不可恢复的失效，包括所有任务失效（如运载火箭发射过程中爆炸，通信卫星所有转发器均不能实施通信功能等）；或导致人员伤亡的失效。

5.5.2 类：致命性失效（critical failure）

将使任务丧失：任务产品不可恢复的失效（如运载火箭未将有效载荷送入预定轨道、入轨偏差大等）；或导致人员、物资损伤的失效。

5.5.3 类：严重失效（major failure）

将使任务降级：部分任务产品丧失，为使任务能继续实施，可能要采取应急措施的失效。

5.5.4 类：轻度失效（minor failure）

对系统与任务无影响，仅轻度影响产品有效使用 and 操作的失效。

5.6 按失效的原因分类

可按导致失效的原因分类：导致失效的原因见4.2。

5.7 按失效所影响的产品层次分类

按失效所影响的产品层次可分为：

- a) 系统级失效；
- b) 分系统级失效；
- c) 设备级失效；
- d) 其它结构层次失效。

5.8 软件异常（失效）的分类

软件异常（失效）的分类要求及内容详见QJ 3026—1998。

5.9 电子元器件失效的分类

电子元器件失效的分类要求及内容详见QJ 1317。

6 危险分类

在安全性分析中，需按危险严重性和危险发生的可能性划分危险的类别和等级。

6.1 危险严重性分类

危险严重性分类是对危险可能造成事故后果严重程度的度量，它表示由于人为差错、环境条件、设计不当、程序错误，或系统、分系统、部件故障可能引起有害后果的严重性。对有关类别的具体规定，应根据具体产品的特点加以明确，并得到供需双方认可。

6.1.1 类：灾难性危险（catastrophic hazard）

可能造成人员死亡、系统完全损失或报废、环境严重破坏的危险。

6.1.2 类：致命性危险（critical hazard）

可能造成人员严重伤害（含严重职业病）、系统或环境较严重破坏的危险。

6.1.3 类：轻度危险（marginal hazard）

可能造成人员一般性伤害（含轻度职业病）、系统或环境一般性破坏的危险。

6.1.4 类：可忽略危险（negligible hazard）

轻于6.1.3所确定的人员伤害、系统或环境破坏的危险。

6.2 危险可能性等级

对具体产品危险可能性等级的规定，要根据产品特点及类似产品历史安全性数据的研究、分析作出定性或定量估计。危险可能性等级的定性度量，可用在产品预期的寿命期中单位时间内发生危险的次数来表示，危险可能性定性等级分类的示例见表1。定量的危险可能性等级通常用发生危险事件的概率或频率来分类。

表1 危险可能性等级示例

说明	等级	单个项目	总体（总体大小由产品定义）
频繁	A	可能经常发生	连续发生
很可能	B	在寿命期内可能发生若干次	频繁发生
偶然	C	在寿命期内可能偶尔发生	发生若干次
很少	D	在寿命期内不易发生，但有可能	不易发生，但有理由预期可能发生
不可能	E	不易发生，可认为不会发生	不易发生，但有可能

6.3 按危险发生时产品所处的研制过程（或寿命剖面）分类

为进行控制，需按危险发生时产品所处的研制过程（或寿命剖面阶段）来分类。研制过程（或寿命剖面阶段）一般可分为：

- a) 制造；
- b) 试验；
- c) 运输；
- d) 装卸；
- e) 贮存；
- f) 使用操作。

7 不合格、失效和危险分类示意图

不合格、失效和危险分类示意图见附录A的图A.1。

附录 A
(资料性附录)
不合格、失效和危险分类示意图

A.1 不合格、失效和危险分类示意图

不合格、失效和危险分类示意图见图A.1

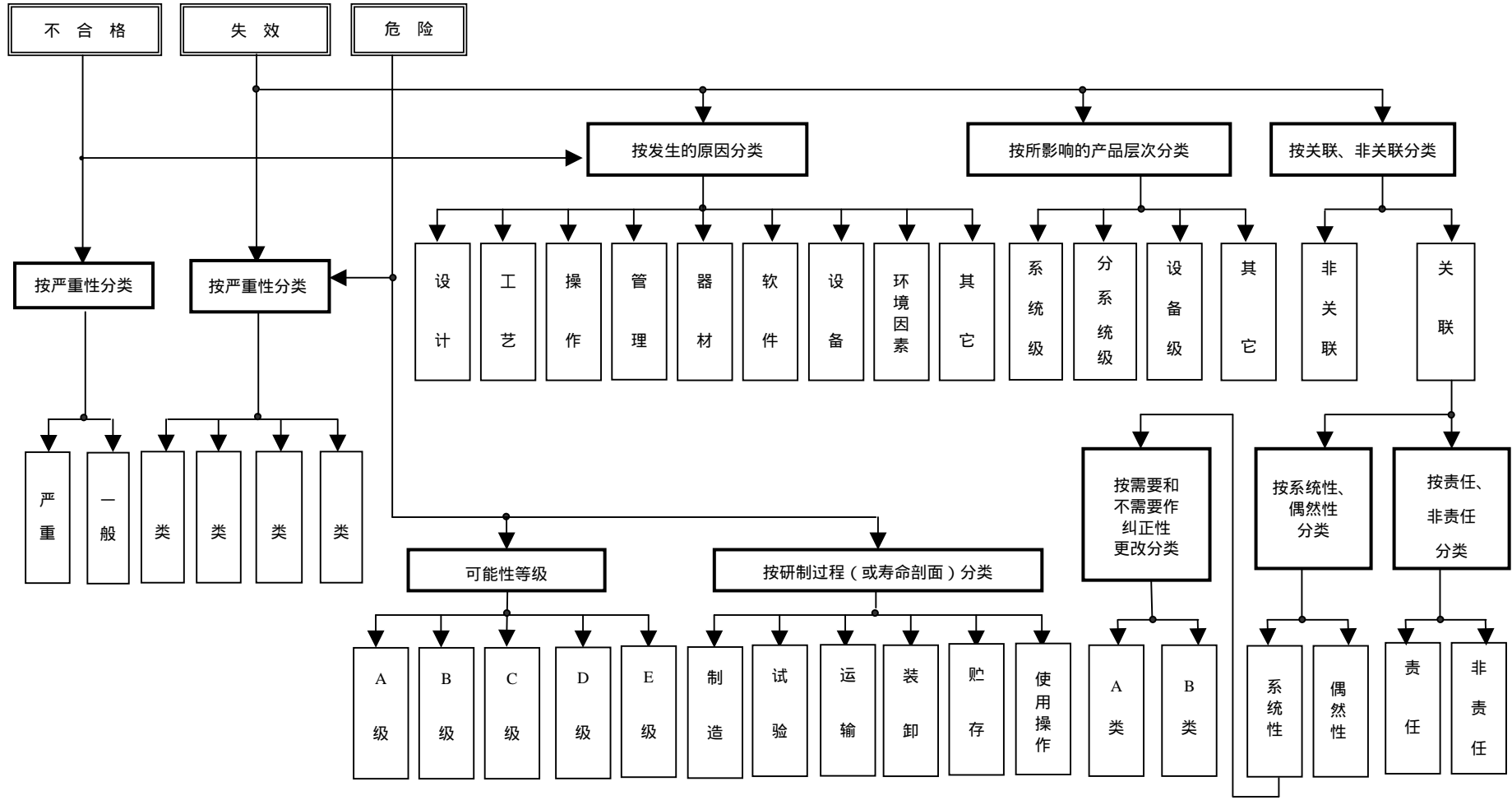


图 A.1 不合格、失效和危险分类示意图

参 考 文 献

- [1] GB/T 11457—1995 软件工程术语
 - [2] GB/T 15174—1994 可靠性增长大纲
 - [3] GB/T 28001-2001 职业健康安全管理体系规范
 - [4] GB/T 19000-2000 质量管理体系 基础和术语
 - [5] GJB179A—1996 计数抽样检查程序及表
 - [6] GJB 1391—1992 故障模式、影响及危害性分析程序
 - [7] GJB 3385—1998 测试与诊断术语
 - [8] GJB/Z 77—1995 可靠性增长管理手册
 - [9] GJB/Z 99—1997 系统安全性手册
 - [10] QJ 1408A—1998 航天产品可靠性保证要求
 - [11] QJ 2236A—1999 航天产品安全性保证要求
 - [12] QJ 2731.1 ~ 2731.12—1995 航天产品质量与可靠性信息分类与代码
 - [13] QJ 3050—1998 航天产品故障模式、影响及危害性分析指南
 - [14] QJ 3139—2001 危险分析方法和程序
 - [15] QJ 9000—1998 航天工业质量管理和质量保证要求
 - [16] MIL—STD—105D 计数抽样检查程序及表
 - [17] MIL—STD—721C 可靠性和维修性术语定义
 - [18] MIL—STD—2074 可靠性试验失效分类
 - [19] ESA—PSS—01—403 危险分析与安全性风险评估方法和程序
 - [20] ECSS—P—001 术语词汇
-

中华人民共和国航天行业标准
航天产品不合格、失效和危险分类
QJ 1544B - 2004

*

中国航天标准化研究所出版
北京西城区月坛北小街2号

邮政编码：100830

北京航标印务中心印刷

中国航天标准化研究所发行

版权专有 不得翻印

*

2004年12月出版

定价：13.00元