ICS 49.020
V 04

中华人民共和国国家标准

GB/T 35439—2017

空间站应用有效载荷安全性、可靠性与维修性保证通用要求

General requirement of safety, reliability and maintainability assurance for the application payloads of space station

2017-12-29 发布　　2018-04-01 实施实施

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

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国科学院提出。

本标准由全国空间科学及应用标准化技术委员会(SAC/TC 312)归口。

本标准起草单位:中国科学院空间应用工程与技术中心。

本标准主要起草人:王功、王伟、方嫚、伏洪勇、刘悦、施建明、刘亦飞。

空间站应用有效载荷安全性、可靠性与维修性保证通用要求

1 范围

本标准规定了空间站应用有效载荷产品类别的划分准则，以及依据产品类别实施安全性、可靠性与维修性(Safety，Reliability and Maintainability，以下简称 SRM)保证工作的通用要求。

本标准适用于空间站、载人飞船、货运飞船等空间飞行器上支持开展空间应用任务的有效载荷。其他空间应用任务有效载荷可参考使用本标准。

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 30114.1 空间科学及其应用术语 第1部分：基础通用

GJB 451 可靠性维修性保障性术语

GJB 1909 装备可靠性维修性保障性要求论证

GJB 2496 载人飞船航天工程术语

QJ 1408 航天产品可靠性保证要求

QJ 2236 航天产品安全性保证要求

QJ 3124 航天产品维修性保证要求

3 术语和定义

GB/T 30114.1、GJB 451、GJB 2496 界定的以及下列术语和定义适用于本文件。

3.1

空间应用有效载荷 space application payloads

装载于空间飞行器平台上，用于执行特定科学实验、科学探测与应用研究的仪器及设备系统。

3.2

SRM 保证 safety，reliability and maintainability assurance

为使人们确信产品达到规定的安全性、可靠性和维修性要求，在产品研制、生产和使用的全过程，所进行的一系列有计划、有组织的 SRM 管理、设计与分析、验证与评价的技术与管理活动，以保证产品以最佳费效比完成所要求的任务。

注：SRM 保证属于产品保证的范畴。

3.3

风险评价指数 risk assessment code；RAC

综合考虑风险事件的后果和发生可能性的危险风险程度的度量指标。

注：通常采用危险风险评价矩阵的方式来表征，纵坐标是风险发生的可能性，横坐标是风险的严重后果。

4 SRM 保证基本原则

有效载荷的 SRM 保证工作遵循以下基本原则：

a) 有效载荷的 SRM 保证工作应在确保安全和应用任务成功的前提下，按照“风险分级、产品分类”的原则，对有效载荷进行分类管理和控制，以实现有效载荷产品 SRM 的适度设计；
b) 有效载荷分类应综合考虑有效载荷的危害性、重要性、研制成本、复杂程度、任务时间、维修需求、保障资源需求以及产品成熟度等风险因素，并对不同风险因素进行综合权衡；
c) 应根据不同的有效载荷产品类别开展相应的 SRM 保证工作，明确 SRM 保证工作项目，各工作项目之间应相互协调，避免重复；
d) 有效载荷 SRM 保证工作应与元器件保证、质量保证以及软件保证等相关工作相协调，结合进行。

5 产品类别的确定

5.1 风险分级

有效载荷风险因素的等级划分见表 1，其中危险风险评价指数的确定见附录 A。

表 1 有效载荷风险因素的分级原则

风险因素		风险等级			
		1 级	2 级	3 级	4 级
关键评价要素[a]	危害性	风险评价指数 1～5，具有不可接受的安全性风险	风险评价指数 6～9，具有不希望发生的安全性风险，需要应用系统决策决定	风险评价指数 10～17，具有可接受，但需进行控制评审的安全性风险	风险评价指数 18～20，具有直接可接受的安全性风险
	重要性	非常重要	重要	普通	次要
	研制成本	极高	高	中等	低
参考评价要素[b]	复杂程度	非常高	高	中等	低
	任务时间	长（连续工作要求≥3 年）	中等（连续工作要求 1～3 年）	较短（连续工作要求 0.5～1 年）	短（连续工作要求≤0.5 年）
	维修需求	不可行或代价巨大，需要多次舱外复杂维修(EVA)	可行但难度很大，需要 EVA 进行维修	可行，需要进行较复杂的舱内活动(IVA)维修	可行，需要简单的舱内活动(IVA)操作
	保障资源需求	大量备件运输需求或在轨可更换单元贮存需求	需要一定量的备件运输或少量在轨可更换单元贮存需求	少量的备件运输需求、不需要在轨可更换单元贮存需求	不需要备件运输、无在轨可更换单元贮存需求
	研制难度	新研产品，采用较多新技术	相似产品，对以往飞行产品进行了较大更改，采用少量新技术	继承性更改产品，对以往成功飞行产品进行适应性改造	继承性成熟产品，经过以往多次飞行试验考核

[a] 关键评价要素是指对有效载荷分类取决定性作用的风险评价要素，有效载荷关键评价要素的风险等级的确定规则如下：

$\Sigma Rc \in [3,5]$，关键要素的综合风险等级为 1 级；

$\Sigma Rc \in [6,8]$，关键要素的综合风险等级为 2 级；

$\Sigma Rc \in [9,10]$，关键要素的综合风险等级为 3 级；

$\Sigma Rc \in [11,12]$，关键要素的综合风险等级为 4 级。

其中，Rc 为关键评价要素的风险等级值，ΣRc 为所有关键要素的风险等级值相加之和。

[b] 参考评价要素的综合风险确定规则为所有参考评价要素中最高的等级，其中，1 级最高，4 级最低。

5.2 有效载荷分类

应根据有效载荷风险因素的分级原则，结合关键评价要素及参考评价要素的综合风险等级对有效载荷产品的类别进行划分，有效载荷的分类准则见表 2。

当关键评价要素的综合风险等级为 1 级、2 级时，可直接根据关键要素的综合风险等级对有效载荷进行分类；当关键评价要素的综合风险等级为 3 级、4 级时，应综合考虑参考评价要素的综合风险等级来对有效载荷进行分类。

表 2 有效载荷的分类准则

有效载荷的类别		关键评价要素综合风险等级			
		1 级	2 级	3 级	4 级
参考评价要素综合风险等级	1 级	第Ⅰ类	第Ⅱ类	第Ⅱ类	第Ⅲ类
	2 级	第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅲ类
	3 级	第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅳ类
	4 级	第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅳ类

6 SRM 要求

6.1 基本要求

有效载荷 SRM 基本要求主要包括：

a) 有效载荷用户应提出明确的 SRM 要求，包括定量要求和定性要求，SRM 要求应纳入研制合同、研制任务书等技术文件中；

b) 有效载荷研制单位应结合有效载荷产品特点，依据合同、研制任务书中规定的 SRM 要求，对 SRM 指标进行逐级分解，转化为系统、分系统和单机的 SRM 设计要求，作为有效载荷研制单位开展 SRM 设计的重要依据；

c) SRM 要求论证应与有效载荷功能、性能指标的论证工作同步进行，并与功能、性能的设计方案进行综合权衡，实现优化设计。

6.2 定量要求

6.2.1 SRM 参数的选择

有效载荷 SRM 参数分为综合参数、安全性参数、可靠性参数、维修性参数，主要参数选择参见表 3。

表 3 有效载荷的 SRM 参数选择参考表

参数类型		参数名称	有效载荷的类别			
			第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅳ类
综合参数		使用可用性	△	△	△	△
安全性		最大可接受风险/事故率	★	★	★	★
可靠性	基本可靠性	平均故障间隔时间（MTBF）	★	★	△	△
	任务可靠性	任务可靠度	★	★	★	★

表 3（续）

参数类型	参数名称	有效载荷的类别			
		第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅳ类
维修性	平均修复时间（MTTR）	★	★	★	★
	最大修复时间	△	△	△	△
	平均预防性维修时间	△	△	—	—
	故障检测率	★	★	△	△
	故障隔离率	★	★	△	△
	虚警率	★	★	△	△
	平均保障延误时间	△	△	△	△
	平均管理延误时间	△	△	△	△
	保障设备满足率	△	△	△	△
	备件满足率	△	△	△	△
注：★为优选参数；△为适用参数；—为不适用。					

6.2.2 SRM 定量要求的确定

有效载荷 SRM 定量要求的确定应按 GJB 1909 的有关规定进行，并遵循以下原则：

a) 有效载荷的 SRM 参数选择和指标确定工作应从科学与应用任务的需求出发，通过系统分析、功能分析、保障性分析等技术，明确顶层的 SRM 参数和指标，并通过逐步分解和反复迭代后提出 SRM 单项要求。

b) 有效载荷 SRM 定量要求的确定应进行可行性分析，全面考虑使用要求、费用、进度、技术水平及相似产品的 SRM 水平等因素，同时，还应重点考虑以下约束条件：

1) 环境条件，包括使用、维修、贮存和运输等环境条件；
2) 与有效载荷保障有关的指挥、控制和通信系统之间的接口；
3) 航天员的作业能力和可用航天员时间；
4) 标准化、系列化、通用化等有关“三化”的总体要求；
5) 保障资源约束，包括上行重量、在轨贮存等；
6) 有效载荷寿命周期费用分析结论，使用和保障费用方面的估算结果。

c) SRM 定量指标的最终确定，应明确相应的环境剖面、任务剖面、主要故障模式和故障判定准则等，同时应明确相应的验证方法，用统计试验验证时应提出置信水平、接收和拒收判据等。

d) SRM 定量指标相互之间应协调匹配，并确保最终确认的 SRM 定量指标与有效载荷设计方案、使用方案和保障方案相协调。

6.3 定性要求

对于不易用定量指标描述或者仅采用定量指标无法全面表征 SRM 要求的有效载荷产品，应明确规定 SRM 定性要求，并进行有效的落实。

示例：采取容错设计，满足“一度故障工作、二度故障安全”的要求；可靠性设计采用成熟技术、简化设计、模块化设计等要求；维修性设计满足可视性、可达性、标准化以及维修操作的便利性等要求。

7 SRM 保证工作项目要求

有效载荷研制单位应根据产品等级确定产品全寿命周期内所应开展的各项 SRM 工作项目，确保产品满足用户规定的 SRM 要求。确定 SRM 保证工作项目时，应遵循以下要求：

a) 有效载荷研制单位应依据有效载荷产品等级，参照 QJ 1408、QJ 2236、QJ 3124 以及本标准表 4 中的相关规定确定有效载荷的 SRM 保证工作项目，Ⅰ类、Ⅱ类和Ⅲ类有效载荷的 SRM 保证工作项目应经上级主管部门审查；

b) 有效载荷研制单位应充分考虑自身产品特点、研制周期和费用等因素，制定有效载荷的 SRM 工作计划(大纲)，保证所有规定的 SRM 工作项目能够按计划顺利开展；

c) 有效载荷研制单位应明确 SRM 保证工作项目实施的责任人，Ⅰ类、Ⅱ类和Ⅲ类有效载荷研制单位应设有专职的 SRM 保证工程师，Ⅳ类有效载荷可依据具体情况由产品设计人员兼任；

d) 有效载荷产品研制单位可根据有效载荷研制的进展情况对有效载荷类别进行更新，有效载荷类别更改时，应对其 SRM 工作项目进行适当的裁剪或补充。

表 4 有效载荷 SRM 保证工作项目选用表

序号	类型	工作项目名称	第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅳ类	工作项目类型
1	协同类工作项目	制定 SRM 工作计划(大纲)	√	√	√	√	管理
2		SRM 专项评审	√	√	△	×	管理
3		SRM 培训	√	√	△	△	管理
4		故障报告及纠正措施系统 FRACAS	√	√	△	△	管理
5		对转承制方的监督与控制	√	√	△	△	管理
6		故障模式影响及危害性分析 FMECA(含维修性信息)	√	√	△	△	分析与设计
7		元器件原材料的选择与控制	√	√	√	√	管理
8		SRM 关键项目确定与控制	√	√	√	√	分析与设计
9		功能测试、包装、装卸、贮存、运输等对产品 SRM 的影响分析	√	√	△	△	分析与设计
10		软件 SRM 设计	√	√	√	√	分析与设计
11		在轨使用数据的收集与分析	√	√	△	△	验证与评价
12	安全性	危险分析	√	√	√	√	分析与设计
13		使用和保障危险分析	△	△	△	△	分析与设计
14		航天员健康危险分析(医学要求分析)	△	△	△	△	分析与设计
15		生物安全防护设计	△	△	△	△	分析与设计
16		激光系统安全性设计	△	△	△	△	分析与设计
17		压力容器/压力系统安全性设计	△	△	△	△	分析与设计
18		电气系统安全性设计	√	√	√	√	分析与设计
19		结构机构安全性设计	√	√	√	√	分析与设计

表 4（续）

序号	类型	工作项目名称	第Ⅰ类	第Ⅱ类	第Ⅲ类	第Ⅳ类	工作项目类型
20	安全性	电池安全性设计	△	△	△	×	分析与设计
21		安全性专项试验	√	√	△	△	验证与评价
22		概率风险评价	√	△	△	×	验证与评价
23	可靠性	可靠性建模、预计与分配	√	√	√	√	分析与设计
24		容差分析	√	√	△	×	分析与设计
25		潜在通路分析	√	√	△	×	分析与设计
26		故障树分析 FTA	√	√	△	△	分析与设计
27		冗余设计	√	√	△	×	分析与设计
28		裕度设计	√	√	△	△	分析与设计
29		力学环境设计	√	√	√	√	分析与设计
30		热设计	√	√	√	√	分析与设计
31		电磁兼容性设计	√	√	√	√	分析与设计
32		抗辐照环境设计	√	√	√	√	分析与设计
33		降额设计	√	√	√	√	分析与设计
34		静电放电防护设计	√	√	√	√	分析与设计
35		抗特殊空间环境设计（原子氧防护设计、太阳紫外辐射防护设计、微重力环境防护设计等）	√	√	√	△	分析与设计
36		环境应力筛选	√	√	√	√	验证与评价
37		可靠性增长试验	√	√	△	△	验证与评价
38		可靠性专项试验	√	√	△	△	验证与评价
39		可靠性评估	√	√	√	△	验证与评价
40	维修性	维修性建模、预计与分配	√	△	△	△	分析与设计
41		维修性分析	√	△	△	△	分析与设计
42		在轨可更换单元（ORU）设计	√	△	△	△	分析与设计
43		维修工效学设计	√	△	△	△	分析与设计
44		维修工具设计	√	△	△	△	分析与设计
45		维修性验证（气浮试验、水槽试验等）	△	△	△	×	验证与评价
46		维修性分析评价	√	√	△	△	验证与评价
注：√为适用；△为根据需要选用；×为不要求。							

附 录 A
（规范性附录）
危险风险评价指数的确定

A.1 危险严重性等级

空间应用有效载荷危险严重性等级分类及定义见表 A.1。

表 A.1 危险严重性分类表

等级	程度	定 义
Ⅰ	灾难的	由于空间应用有效载荷的故障将导致： a） 人员死亡； b） 载人航天器完全损失或报废； c） 环境严重破坏
Ⅱ	严重的	由于空间应用有效载荷的故障将导致： a） 人员严重伤害（含严重职业病）； b） 载人航天器或环境较为严重破坏； c） 载人航天器或科学实验平台关键设备或功能的暂时性丧失，需要进行紧急的在轨维修，并且有可能导致飞行任务中止，航天员避险或紧急撤离； d） 应用载荷（或科学实验平台）完全损失报废，或者重大应用任务完全失败
Ⅲ	轻度的	由于空间应用有效载荷的故障将导致： a） 人员的轻度伤害（含轻度职业病）； b） 航天器系统非关键功能的暂时性丧失或应用任务部分失败，需要进行专门的在轨修复性维修或更换
Ⅳ	轻微的	轻于Ⅲ类的人员伤害或轻于Ⅲ类的系统损坏，不影响任务完成

A.2 危险可能性

危险可能性可在产品预期的寿命期中单位时间内产生危险的次数来表示。可通过对类似产品历史安全性数据的研究、分析做出定性或定量的估计。危险可能性的定性等级分类见表 A.2。

表 A.2 危险可能性分类表

说明	等级	产品个体	产品总体（或系统）
频繁	A	在产品寿命期内可能频繁发生，发生概率大于 10^{-1}	连续发生
			对空间应用有效载荷产品意味着在其飞行期间可能出现一次或多次

表 A.2（续）

说明	等级	产品个体	产品总体(或系统)
很可能	B	在产品寿命期内发生若干次，发生概率小于 10^{-1} 但大于 10^{-2}	经常发生
			对空间应用有效载荷产品意味着在其一次飞行中可能不发生，但在其使用期间可能发生数次
偶然	C	在产品寿命期内可能有时发生，发生概率小于 10^{-2} 但大于 10^{-3}	发生若干次
			对空间应用有效载荷产品意味着在其使用期间发生一次或可能不发生
很少	D	在产品寿命期内不易发生，但有可能发生，发生概率小于 10^{-3} 但大于 10^{-6}	不易发生，但有理由预期可能发生
			对空间应用有效载荷意味着在其使用期间发生可能是一种例外现象
不可能	E	不易发生，可假定不会发生，发生概率小于 10^{-6}	不易发生，但有极小可能发生
			对空间应用有效载荷意味着在其全部使用期间不可能发生

A.3 风险评价指数

空间应用有效载荷应综合危险严重性和危险可能性两方面因素来确定风险评价指数，并以此为依据进行风险决策。

危险风险评价指数见表 A.3。

表 A.3 危险风险评价指数表

可能性等级	严重性等级			
	Ⅰ(灾难的)	Ⅱ(严重的)	Ⅲ(轻度的)	Ⅳ(轻微的)
A(频繁)	1	3	7	13
B(很可能)	2	5	9	16
C(偶然)	4	6	11	18
D(很少)	8	10	14	19
E(不可能)	12	15	17	20

A.4 风险评价决策管理

有效载荷研制过程中应通过安全性要求的逐级分解、危险识别、风险评价、已识别危险的处理及危险结果等活动进行风险管理，风险管理的原则如下：

a) 对已识别的风险指数较高的潜在危险应有相应的消除或控制措施，当所采取的措施不能将危

险后果的严重程度降低到可接受水平时，应考虑减少危险事件发生的概率；

b） 应采纳所有能够减少潜在风险而又不会降低可靠性的建议；应采纳能够减少潜在危险的发生概率而又不会增加危险后果严重程度的提议；

c） 每项残余危险及其未能完善解决的原因应记录在案并向指定的危险跟踪监控部门报告。

根据风险指数进行风险评价决策准则，风险接受准则见表 A.4。

表 A.4 风险接受准则

风险指数	风险水平	评价准则
1～5	高	不可接受，必须采取措施予以消除或降低，使其达到可接受的程度
6～9	严重	有条件的接受，并采取针对性的措施
10～17	中	经评审或审批后可接受
18～20	低	可接受