改进FMECA在空间电源分系统中的应用

孔雷星,冷学敏,马季军,葛茂艳,王 田
(上海空间电源研究所,上海200245)

摘 要: 故障模式、影响及危害性分析(FMECA)方法广泛应用于航天领域,并较早地形成了航天领域内的FMECA规范,基本满足型号常规使用的要求。但是,随着航天产品的日益复杂及高可靠性的要求,FMECA规范已无法完全适用,尤其是FMECA工作的有效性和全面性有待进一步研究。本文从三方面提出改进FMECA的方法程序,包括改进功能和结构分析方法,完善FMECA表格,增加发生可能性的级别,同时以电源分系统的分流调节器为例,验证改进后FMECA方法程序的可行性。分析结果显示:改进后的FMECA分析层级清晰,表格填写规范,故障模式和故障原因分析更全面,更有利于发现薄弱环节,并有针对性地指导产品开展设计改进,提高产品可靠性。

关键词: 故障模式、影响及危害性分析(FMECA); 薄弱环节; 空间电源分系统; 发生可能性; 可靠性

中图分类号: TN 911.73; TP 391.9 **文献标志码:** A **DOI:** 10.19328/j.cnki.1006-1630.2021.01.018

Application of an Improved FMECA in Space Power Subsystem

KONG Leixing, LENG Xuemin, MA Jijun, GE Maoyan, WANG Tian
(Shanghai Institute of Space Power-Sources, Shanghai 200245, China)

Abstract: Failure mode, effect and criticality analysis (FMECA) method is widely used in the aerospace. The conventional FMECA specification in the aerospace is formed earlier, which basically meets the requirements of general application of spacecrafts. However, with the increasing complexity and requirement of higher reliability for aerospace products, conventional FMECA specification can't be completely applied. Especially, the effectiveness and comprehensiveness of FMECA need to be further studied. In this paper, a method of improving FMECA is proposed based on three aspects, including improving function and structure analysis method, improving FMECA table and adding the level of probability of occurrence. Moreover, the shunt regulator of the power subsystem is given as an example to show the feasibility of the improved FMECA method. The analysis results show that the improved FMECA's analysis level is clearer, the form is more standardized, and the failure mode and reason analysis are more comprehensive. Therefore, the improved FMECA is more conducive to find the weakness, guide the product design and improvement , and improve the product reliability.

Key words: failure mode, effect and criticality analysis (FMECA); weakness; space power system; probability of occurrence; reliability

0 引言

故障模式、影响及危害性分析(Failure Mode, Effect and Criticality Analysis,FMECA)是分析产品中每一个可能的故障模式并确定其对产品及上层产品所产生的影响,以及把每一个故障模式按其影响的严重程度予以分类的一种分析技术[1]。FMECA在FMEA的基础上增加了危害性分析(CA)的内容。FMEA的主要作用是找出潜在的薄弱环节,尽可能早地发现设计、工艺过程中的各种缺陷,并提出改进措施,从而提高设计质量。20世纪50年代,

收稿日期: 2019-11-30; **修回日期:** 2020-01-13
基金项目: 上海市科技人才计划项目(18XD1422200)
作者简介: 孔雷星(1987—),女,硕士研究生,工程师,主要研究方向为空间电源可靠性设计分析。

FMEA产生于美国航空业内，到60年代正式用于美国航天领域。80年代初，我国才开始引进FMEA，相继颁布了一系列国家标准、军用标准等[2-6]。FMECA方法也广泛应用于各行各业[7-12]，例如：质量安全管理、地铁车辆、医学、航空、航天和烟草企业等。更有学者对FMECA的方法进行了深入研究[13-15]，例如接口FMECA、模糊FMEA等。目前航天领域引用最多、使用最广泛的为GJB/Z 1391—2006《故障模式、影响及危害性分析指南》，主要介绍了功能及硬件FMECA、软件FMECA、损坏模式及影响分析、过程FMECA的程序和方法，以及由中国空间技术研究院颁发的Q/W 1364—2012《航天器产品故障模式及影响》，主要介绍了不同层级产品开展设计FMEA及过程FMEA的程序及方法，并详细介绍了冗余系统开展FMEA的方法。依据以上两个标准，型号中开展设计FMECA基本能够满足工程的要求。但是，在型号工作中，FMECA工作并未完全发挥其作用，原因包括：1）原有的功能层次与结构层次框图主要适用于具有简单连接关系的系统中，难以满足功能及连接关系越来越复杂的系统应用；2）原有的FMECA主要侧重于定性故障模式、故障原因等分析，对于定量分析缺乏有效的操作指导；3）原FMECA中故障模式发生可能性划分层级较粗，而现阶段产品可靠性要求及生产制造水平等越来越高，较粗的划分层级无法满足使用需求；4）产品与产品之间的接口通常被认为高可靠而不进行分析，或由于接口的复杂性导致故障识别不到位，不全面。基于上述原因，FMECA工作在型号实际应用中并未得到从上至下的重视，即使FMECA工作主观上被重视了，但部分设计师对FMECA工作方法和程序不熟练，对产品或系统未进行分析就着手填写FMECA表格，导致分析层级混乱，表格填写不规范，故障模式和故障原因分析不全。

针对以上4个突出的问题，本文提出改进FMECA的方法程序，包括3方面：1）改进产品的功能和结构分析方法，确定FMECA的分析范围、识别功能及其设计要素；2）完善FMECA分析表格，增加功能的量化指标要求，增加现行控制措施的分类；3）增加发生可能性的级别，通过增加继承产品的失效情况可更有效地识别故障发生可能性，便于判断采取改进措施后是否对设计提供了帮助。

1　改进FMECA方法

1.1　确定分析范围

FMECA分析的首要工作是确定分析边界，即确定哪些产品需要开展FMECA，哪些产品不开展，主要通过产品结构树和结构框图这两种方法配合确定分析范围。

产品结构树是按照树状图从上至下梳理产品的硬件组成，需要开展分析的产品用实框表示，不需开展分析的产品用虚框表示，如图1所示。是否开展FMECA分析的原则通常包括以下两项：1）外购件产品不需要开展分析，如商用电脑、集成芯片、霍尔传感器、螺钉等。原因是对于使用者来说，只要外购件产品的功能和性能满足要求，其接口能够与系统匹配，不必了解外购件产品的内部组成关系，因此不需进行分析。2）功能单一且设计要素低（即性能指标少）的产品不需要开展分析，例如电连接器、导线、产品结构框架等。

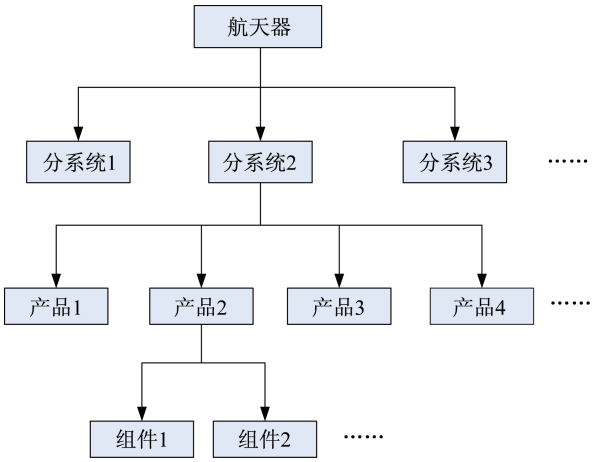

图1　结构树示意图

Fig.1　Structure tree diagram

结构框图是识别产品内外部及接口之间的交互关系的一种图形，它既可以反映产品结构内部各零件之间的关系，也能反映产品与外部系统之间的关系，如图2所示。

结构框图中的接口关系包括物理空间关系、能量传递关系、信息传递关系、物质交换关系和人机交互关系。对于空间电源系统来说，除了物质交换关系，其余的接口关系都涉及。

结构框图中的连接方式没有特定的要求，但需要对每个连接关系进行准确的说明。通常，若两个

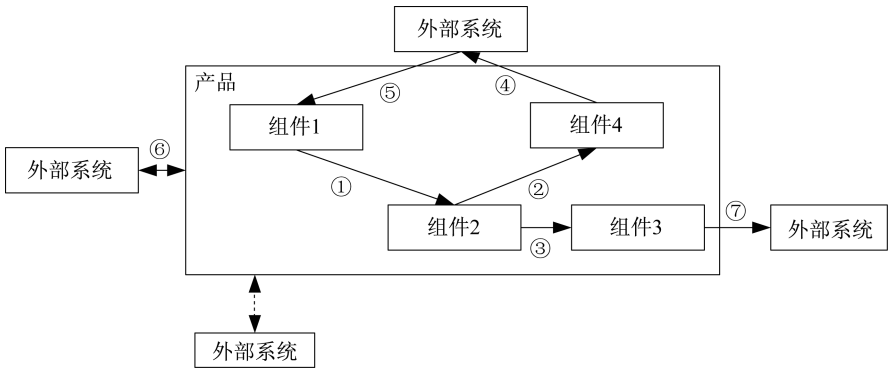

图 2 结构框图示意图

Fig.2 Structural block diagram

产品之间只有物理空间关系,用不带箭头的实线条表示,若没有物理空间关系,用虚线条表示,用箭头表示两个产品之间的物质或能量或信息的传递方向。图中的数字表示有物理空间关系及其他接口关系的具体表现形式,例如螺栓连接、压装、焊接、勾焊、导线连接、电连接器连接、热传递、电能传递、信息传递等,并列表说明。

通过结构框图可以清楚地表示产品与产品之间的接口关系,即使某产品不进行FMECA分析,但其接口也能被表示出来,不会遗漏任何的接口。

1.2 功能及要求分析

FMECA分析的另一项重要工作是针对分析对象开展功能分析,明确产品的功能及参数指标要求,主要采用功能树和功能框图这两种工具来识别功能、功能的交互关系及功能的冗余情况。

功能树分析以产品结构树为基础,以分析对象的功能为核心,向上和向下各分析一层,如图3所示。功能树中需要关注以下几点:1) 分析对象的每一个功能单独画一棵功能树,最后将上一层功能相同的功能树合并,为分析对象的上级产品开展FMECA提供信息;2) 功能树中需要明确表征该功能的参数指标;3) 结构框图中每个产品与产品之间的接口关系均要反映在功能树中,例如图中的组件1和组件2;4) 功能树中需要给出两个或多个没有交互关系(没有接口关系)的产品共同完成同一功能的情况,例如图中的组件3和组件4;5) 从功能树中将分析对象的功能及参数指标要求进行汇总,并形成表格。

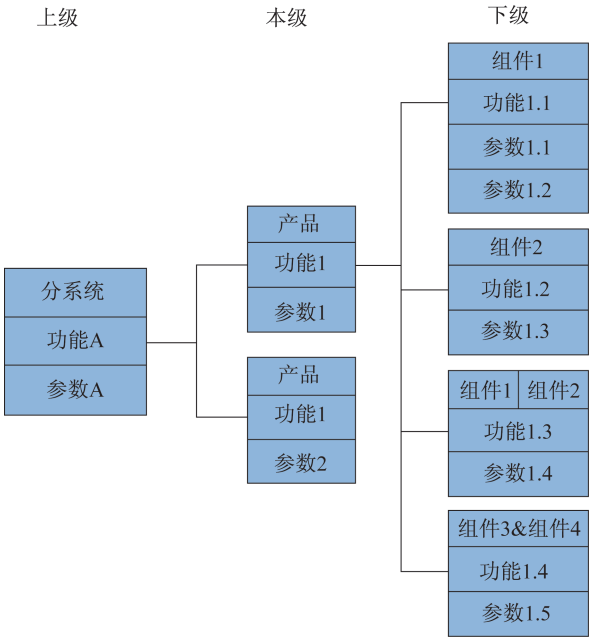

图 3 功能树示意图

Fig.3 Function tree diagram

功能框图表示各功能之间的界面和接口的序列关系(输入/输出)。以功能树为基础,首先对分析对象(本级产品)的功能之间关系用功能框图表示出来,即用一个顶层框图来表示被分析的整个项目,再将每个本级功能的下级功能用功能框图表示出来,即用若干张图表示顶层框图中某一确定功能的细节部分,功能框图示意图如图4所示。

与结构框图类似,功能框图中的接口关系包括能量传递关系、信息传递关系、物质交换关系,可以用不同的线型表示不同的接口关系。功能框图中需要关注以下几点:1) 若建立一系列按层次划分的功能框图,则每个框图应与相邻层次框图保持一致性;2) 某一个功能框图只能对应于与功能树相应的

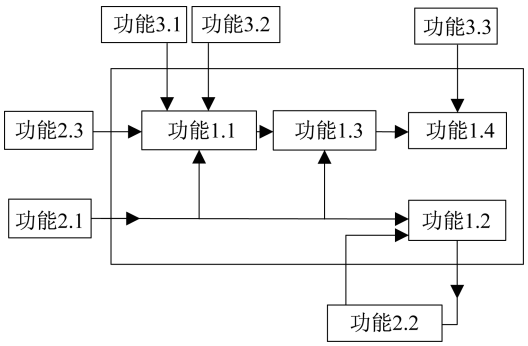

图 4　功能框图示意图

Fig.4　Functional block diagram

同一层次；3）功能框图应能描述出系统的冗余结构，为填写FMECA表格中的预防措施奠定基础；4）针对不同的任务阶段和工作模式，航天器产品应建立不同的功能框图来表示全任务阶段的各个状态。

1.3　FMECA表格改进

经过对产品的结构和功能分析，下一步可以填写FMECA表格。为了更加凸显FMECA分析的作用，在现有型号表格的基础上进行完善，见表1。

表 1　FMECA表格

Tab.1　FMECA form

序号1	产品或功能标志2	功能描述3	性能要求(量化)4	故障模式5	任务阶段及工作模式6	故障影响7			严酷度8	发生可能性9	风险评价指数10	单点故障11	故障原因12	故障检测方法		现行控制措施		建议改进措施17	飞行过程补偿措施18	备注19
						局部影响	高一层影响	最终影响						飞行过程检测方法13	地面检测方法14	设计预防/纠正措施15	过程控制措施16			

表1中，新增了第4、16列，下面对重要列进行详细说明。

第2列：填写分析对象。

第3列：填写从功能树中识别的功能。

第4列：填写从功能树中识别的功能参数指标。

第5列：功能参数指标的反面即为故障模式。

第6列：给出产品的任务阶段及具体的工作状态。

第7列：从其相关联的系统/子系统/产品/零部件、生产制造、使用用户等角度填写影响，并可从故障现象及便于严酷度打分的角度进行描述。

第8列：针对最终影响结果对照严酷度等级分类表进行填写。

第9列：增加发生可能性的层级，便于进行采取措施前后的对比，见表2（参考汽车行业FMEA手册[3]）。

表 2　故障发生频度[6]

Tab.2　Failure frequency[6]

等级		程度	发生频度(文字)	发生频度(量化)
A		经常	没有前期历史的新技术/新设计	≥1/10
B	B1	有时	在工作循环/操作内，对于新设计、新应用或变更，失效不可避免的	1/20
	B2		在工作循环/操作内，对于新设计、新应用或变更，失效是可能的	1/50
	B3		在工作循环/操作内，对于新设计、新应用或变更，失效是不确定的	1/100
C	C1	偶然	相似设计或在设计模拟/测试时频繁失效	1/500
	C2		相似设计或在设计模拟/测试时偶尔失效	1/2 000
	C3		相似设计或在设计模拟/测试时个别失效	1/10 000
D	D1	很少	几乎相同设计，或者在设计模拟/测试时仅有的个别失效	1/100 000
	D2		几乎相同设计，或者在设计模拟/测试时没有失效	1/1 000 000
E		极少	通过预防控制措施消除失效	通过预防控制措施消除了失效

第10列:根据严酷度和新的发生可能性定义新的风险评价指数,见表3,风险指数对应的处理原则见表4。

表3 风险指数[4]

Tab.3 Risk index[4]

故障频度		严酷度			
		Ⅰ	Ⅱ	Ⅲ	Ⅳ
A		1	3	7	11
B	B1	2	4	9	12
	B2	3	5	10	13
	B3	4	6	11	14
C	C1	5	7	12	15
	C2	6	8	13	16
	C3	7	9	14	17
D	D1	8	10	15	18
	D2	9	11	16	19
E		12	15	17	20

表4 风险指数对应的处理原则[4]

Tab.4 Principles of risk index[4]

风险指数	处理原则
1～5	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	有条件的接受,并采取针对性的措施
10～17	经评审或审批后可接受
18～20	可接受

第11列:给出会引起系统故障,且没有冗余或替代的操作程序作为补救的产品故障,若符合该定义,填写“Y”,若不符合该定义,填写“N”。

第12列:故障原因可从功能树中识别,为下一层产品的功能参数要求的反面及下一层产品接口的功能参数要求的反面,也可从故障现象进行定性描述。

第13列:给出在任务执行时能够表征该故障的遥测参数(包括参数代号及参数名称)。

第14列:给出产品在地面测试阶段能够表征该故障的参数或其他手段。

第15列:针对故障原因提出可以指导设计的措施和方法,例如失效安全设计、设计和材料标准、设计防错、模拟研究(概念分析、建立设计要求等)。

第16列:针对故障原因和故障模式提出可以检查设计的措施和方法,例如设计评审、试验验证、模拟研究(设计验证)、使用相似部件的原型、关强点设置等。

第17列:从3个维度考虑。1)通过更改设计降低严酷度等级;2)通过设计修改或控制手段,消除或减少失效原因出现的可能(例如实行设计防错措施、优化设计结构、冗余设计、裕度设计、修订材料规格);3)改进检查设计的方法,将检查设计的工作提前(例如试验优化、在产品设计前期进行检查、采用更高级的检查方法)。

第18列:填写产品在执行任务期间,针对故障可采取的应对措施。

第19列:其他需要说明的事项。

2 改进FMECA方法在空间电源分系统的应用案例

2.1 空间电源分系统的特点

空间电源分系统的特点包括:

1)工作环境严酷。

空间电源分系统既有舱外设备也有舱内设备,舱内设备处于失重的环境,舱外设备处于高层大气、地磁场、天体应力场、高能带电粒子、空间等离子体、高低温交变、原子氧、微流星和空间碎片等环境[2],这些环境对电源分系统的主要影响为温度、辐射损伤、机械损伤、化学损伤、表面充电放电等,这些影响都会加速电源分系统的机电设备和承载结构失效。

2)分系统设备类型多、小子样问题突出。

空间电源分系统主要功能是给航天器提供电能,但其设备类型包含4类:机电类、电子电器类、机构类和电化学类,需要采取不同的可靠性分析手段满足总体的要求。空间电源分系统的设备基本上是单件或小批量生产,其可靠性数据不够充分,可靠性特征不易掌握。

3)工作周期长、可靠性要求高。

为了配合航天器,空间电源分系统在轨工作周期长,对各设备的可靠性提出了较高的要求,给设计工作带来了巨大的挑战。

4)在轨可维修。

由于航天器在轨时间长,空间电源分系统在轨可维修是为了适应航天的发展最新提出的要求,其维修方案、维修时机、维修内容和维修手段等仍处于摸索阶段,可借鉴的资料较少。另外,由于空间

环境的影响，空间电源分系统维修时间较长、维修难度较大、维修风险较高，这些都给在轨可维修带来很多不确定的因素。

5）储能电池要求高。

未来的空间电源分系统将采用锂离子蓄电池作为储能电池，不再有应急电源作为在阴影区出现功率峰值时的电能补充，因此，需要避免出现此种情况，增加电池的功率。

6）安全性问题突出。

目前空间电源分系统采用高电压母线控制，万一发生漏电事故，将有可能导致设备和人员的损伤。在设备的维修过程中，也存在触及高压的危险。

2.2　确定分析范围

以某航天飞行器电源分系统的分流调节器为例，它主要包括供电分流电路、二次电源电路、母线滤波电路、参数测量电路、底板和汇流铜条，分流调节器产品组成图如图5所示。产品的组成关系主要包括：1）供电分流电路、母线滤波电路、二次电源电路及汇流铜条由于发热量较大，通过螺接的方式安装在底板上；2）供电分流电路、母线滤波电路、二次电源电路均需要进行参数测量，因此参数测量电路需要将产品的参数传输给电源分系统的电源管理器及整器的数管分系统；3）供电分流电路通过电缆接受太阳电池翼的100 V发电功率，并通过汇流铜条将100 V发电功率输出给下游设备——母线滤波器；4）母线滤波器将MEA信号通过电缆连接器传输给供电分流电路；5）汇流铜条通过机内电缆将100 V发电功率传输给二次电源电路，二次电源电路为供电分流电路和参数测量电路提供±12 V。

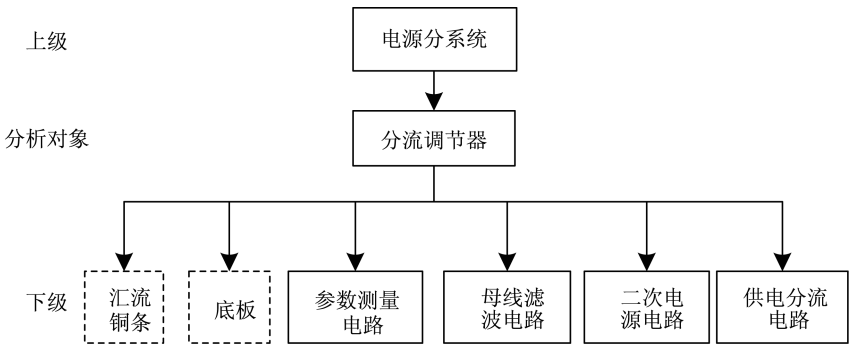

图5　分流调节器产品结构树

Fig.5　Structure tree diagram of shunt regulator product

产品具体的结构框图如图6所示，内外接口交互关系表见表5。

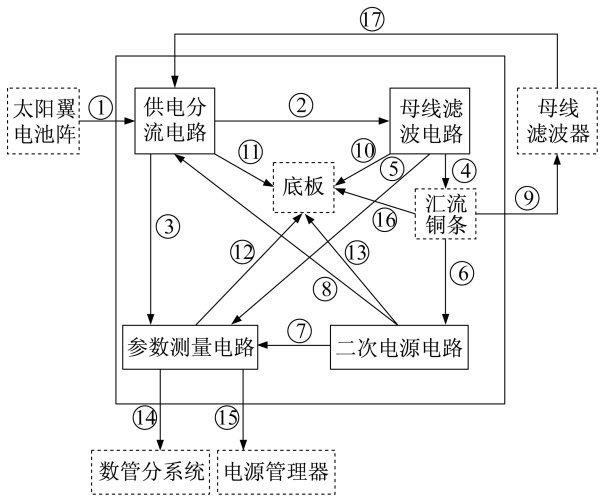

图6　分流调节器结构框图

Fig.6　Structural block diagram of shunt regulator product

2.3　功能及要求分析

分流调节器主要实现3个功能：分流功能、供电功能和参数测量功能，具体见表6。3个功能的交互关系如图7所示。

分流功能需要由供电分流电路、二次电源电路、底板这3部分来完成，功能量化要求包括：1）分流MEA控制电压域为6.3～9.0 V；2）15路分流供电电路，每路分流能力为7.2 A；3）母线电压维持在105～107 V；4）产品的工作温度维持在5～35 ℃。分流功能树如图8所示。

2.4　FMECA表格填写

以分流调节器的分流功能为例，填写FMECA表格。根据产品结构框图及功能分析，分流调节器本级功能的反面即为故障模式，下级功能的反面即为故障原因，见表7和表8。

表 5 分流调节器接口交互关系表

Tab.5 Interface interaction relationship table of shunt regulator product

序号	交互关系	备注
①	电缆连接器连接，电能传递	供电分流电路通过机内电缆焊接到电连接器插座内
②	机内导线焊接，电能传递	—
③	机内导线焊接，信号传递	—
④	机内导线焊接，电能传递	—
⑤	机内导线焊接，信号传递	—
⑥	机内导线焊接，电能传递	—
⑦	机内导线焊接，电能传递	—
⑧	机内导线焊接，电能传递	—
⑨	电缆连接器连接，电能传递	汇流铜条通过机内电缆焊接到电连接器插座内
⑩	压接及螺接，热传递	—
⑪	螺接，热传递	—
⑫	螺接	—
⑬	螺接，热传递	—
⑭	电缆连接器连接，信号传递	参数测量电路通过机内电缆焊接到电连接器插座内
⑮	电缆连接器连接，信号传递	
⑯	绝缘螺接，热传递	底板和汇流铜条之间用绝缘板隔离
⑰	电缆连接器连接，信号传递	MEA 信号

表 6 分流调节器功能分析表

Tab.6 Function analysis table of shunt regulator

序号	分析对象	功能	要求
1	分流调节器	分流功能	15路分流电路，每路分流能力不小于7.2 A
2		供电功能	具备全供电的能力，总电流输出不小于98 A
3		参数测量功能	共31个参数，参数测量范围均满足要求

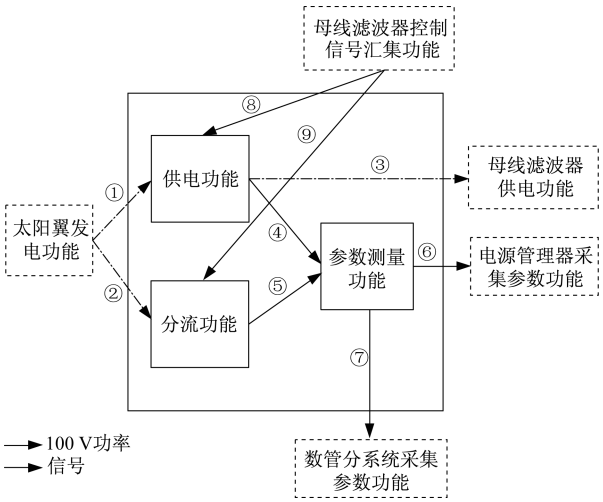

图 7 分流调节器功能框图

Fig.7 Functional block diagram of shunt regulator

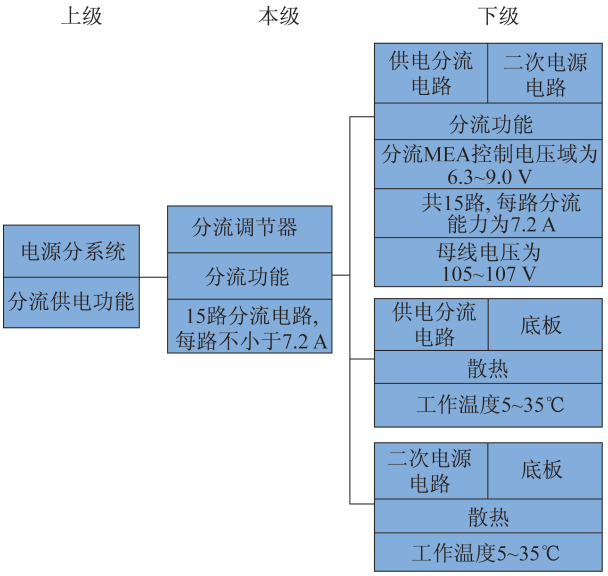

图 8 分流功能树

Fig.8 Shunt function tree

根据表 2 和表 3 的定义，确定该故障模式的发生可能性为 C3，风险评价指数为 7。

表 7 FMECA 分析 1

Tab.7 FMECA analysis 1

序号	产品或功能标识	功能描述	性能要求	故障模式	任务阶段及工作模式	故障影响			严酷度	发生可能性	风险评价指数	单点故障
						局部影响	高一层影响	最终影响				
1	分流调节器	分流功能	具备15路分流能力，每路分流能力不小于7.2 A	15路均无法分流	在轨运行光照区	分流功能丧失	电源分系统无法分流	母线电压高于 107 V，引起下游负载烧坏	I	C3	7	Y

表 8　FMECA 分析 2

Tab.8　FMECA analysis 2

故障原因	故障检测方法		现行控制措施		建议改进措施	飞行过程补偿措施
	飞行过程检测方法	地面检测方法	设计预防/纠正措施	过程控制措施		
供电分流电路故障使分流MEA控制电压域不在6.3～9.0 V	参数监测	参数监测	1）建立仿真模型进行模拟； 2）器件进行I级降额设计； 3）每路分流电路设置一路控制信号	1）开展电性能测试； 2）原理图设计评审； 3）将重要关键器件列为关重件	1）供电分流电路进行冗余设计； 2）增加1台分流调节器	1）将太阳翼帆板偏置； 2）增加负载
二次电源供电电路故障使分流MEA控制电压域不在6.3～9.0 V	参数监测	参数监测	1）建立仿真模型进行模拟； 2）器件进行I级降额设计； 3）采用2组2并热冗余设计	1）开展电性能测试； 2）原理图设计评审	1）采用2组2热1冷的冗余设计； 2）增加1台分流调节器	1）将太阳翼帆板偏置； 2）增加负载
二次电源电路给供电分流电路供电的机内电缆断路使分流MEA控制电压域不在6.3～9.0 V	参数监测	参数监测	1）建立仿真模型进行模拟； 2）器件进行I级降额设计； 3）机内电缆采用2并传输	1）开展电性能测试； 2）原理图设计评审	1）增加电缆焊点检查； 2）增加1台分流调节器	1）将太阳翼帆板偏置； 2）增加负载
二次电源电路与底板的接触不良造成热传递不佳使产品不在正常工作温度内	参数监测	参数监测	1）建立仿真模型进行模拟； 2）器件进行I级降额设计； 3）产品封盖检查； 4）在功率器件上粘贴温度传感器	1）开展电性能测试； 2）开展力学、温度试验； 3）开展热仿真验证	1）规定螺钉拧紧的力矩； 2）更换为热传导效果更好的螺钉； 3）增加1台分流调节器	1）将太阳翼帆板偏置； 2）增加负载
供电分流电路与底板的接触不良造成热传递不佳使产品不在正常工作温度内	参数监测	参数监测	1）建立仿真模型进行模拟； 2）器件进行I级降额设计； 3）产品封盖检查； 4）在功率器件上粘贴温度传感器	1）开展电性能测试； 2）开展力学、温度试验； 3）开展热仿真验证	1）规定螺钉拧紧的力矩； 2）更换为热传导效果更好的螺钉； 3）增加1台分流调节器	1）将太阳翼帆板偏置； 2）增加负载

从表8中可以看出，故障原因中不仅分析了电路模块引起的故障，并且分析了接口引起的故障，只要在功能和结构分析中对接口的分析是全面的，那么在FMECA分析表中必会反映出接口。同时，根据不同的故障原因提出了不同的改进建议，目的是保证指标参数不发生错误，从而确保功能执行的正确性，最终提高产品的可靠性。

2.5　FMECA结果分析

分流调节器是航天器电源分系统中必不可少的产品，它的可靠与否可决定电源系统的工作寿命长短，通过FMECA分析，得到以下结果：1）MEA控制电压域和工作温度是制约分流功能的关键参数；2）改进措施中不仅考虑了设计，通过接口识别还增加了工艺过程实施；3）按照新的发生可能性表，故障发生可能性从一律的“E”变为了“C3”。

3　结束语

本文针对现有FMECA方法存在的两个缺陷——无法有效指导设计改进和接口分析不到位，从3个方面提出了改进方法：改进产品功能和结构分析方法，完善FMECA分析表格和增加发生可能性的级别，并以分流调节器为例进行了逐一分析。从分析结果可知，FMECA分析层级更加清晰，表格填写更加规范，故障模式和故障原因分析更加全面，指标量化更有利于发现设计薄弱环节，更有针对性地指导产品开展设计改进，弥补了现有FMECA的缺陷，有利于产品提高可靠性。

参考文献

[1] 康锐，石荣德.FMECA技术及其应用[M].北京：国防工业出版社，2006：12-21.

[2] 都亨，叶宗海.低轨道航天器空间环境手册[M].北京：国防工业出版社，1999.

[3] 康锐，石荣德.故障模式、影响及危害性分析指南：GJB/Z 1391[S].中国人民解放军总装备部，2006.

[4] 任立明，李福秋.航天产品故障模式、影响及危害性分析指南：QJ3050A[S].国家国防科技工业局，2011.

[5] 胡剑敏，徐银波.型号设计故障模式影响分析（DFMEA）指南：Q/RJ/Z122[S].中国航天科技集团公司第八研究院，2017.

（下转第156页）