

“天宫一号”目标飞行器系统级自主安全设计

李智勇

(中国空间技术研究院 载人航天总体部, 北京 100094)

摘要: 为确保载人飞行器在长期飞行中的设备安全以及短期飞行中航天员的安全, 需要从系统层面进行自主安全设计, 使航天器在出现地面无法快速反应的故障时能够启动安全模式进行自我保护。文章以能源安全设计为主对“天宫一号”目标飞行器系统级自主安全设计进行了论述, 总结了设计经验, 对后续型号的设计提出了建议。

关键词: 目标飞行器; 飞行安全; 总体设计; 能源系统

中图分类号: V57; V525

文献标识码: A

文章编号: 1673-1379(2011)06-0525-04

DOI: 10.3969/j.issn.1673-1379.2011.06.004

0 引言

“天宫一号”目标飞行器是长期在轨飞行、短期有人照料的低轨载人飞行器。与以往多次载人航天任务中的密集测控覆盖不同, “天宫一号”在长期飞行过程中测控覆盖率较低, 因此如何确保长期在轨期间平台的安全是决定飞行任务成败的关键内容之一。在分系统自主控制的基础上, 需要针对飞行器关键特性, 进行系统级的自主安全设计。

1 系统级自主安全设计的定义

自主安全设计是指不需要地面的直接干预, 飞行器依靠自身功能对在轨产生的故障自主进行处置或者隔离, 以消除故障或者降低故障影响, 为后续地面干预提供条件的设计。目前我国飞行器在设计上采用了多种安全性措施, 比如熔断器、过压保护、过流保护等。

系统级的自主安全设计是结合飞行器任务特点, 从系统角度对影响飞行器平台安全的相关分系统功能进行自主安全设计。在自主安全状态下, 一旦发生影响平台安全且实时性处理要求较高的严重故障, 飞行器能够自主进入安全模式, 进行一系列的处置, 以确保整器安全。

我国一些空间飞行器开展了系统级的自主安全设计, 如二代导航卫星综合电子系统的自主健康管理: 综合电子系统中采用卫星管理单元(SMU)

模块集中管理, 由接受卫星管理单元控制的卫星控制接口单元(SCIU)实施对分系统的管理。SMU通过既定的规则, 对整星故障进行系统重构或将卫星切换到整星级别的安全模式。

深空探测航天器常采用的自主管理主要有温度控制、供电控制、蓄电池充放电管理控制及重要部件通断电控制等。如我国月球探测卫星开展了数传设备自主关机、温度控制、充放电控制和旨在节省能源的自主应急控制等自主管理设计。

2 “天宫一号”系统级自主安全设计

“天宫一号”的平台由能源系统、通信系统、姿轨控系统、环境和热控制系统以及对接支持系统等组成, 其中前4个系统是系统级安全设计主要考虑的对象。这些系统失效的后果都很严重, 也是近年来导致航天器故障的主要原因。这些系统的严重故障模式包括能源不能保障、飞行器姿态翻滚、推进剂在测控区外泄漏殆尽以及载人环境控制受到威胁等。

系统级自主安全设计的原理是根据任务需求或者系统特点建立飞行器系统级的安全控制模型, 通过实际飞行参数驱动存储在中心计算机中的控制模型; 当出现符合故障预案中的条件时, 启动安全控制程序并由执行单元执行, 如图1所示^[1]。下面以能源安全模式设计为主进行介绍。

收稿日期: 2011-10-28; 修回日期: 2011-11-24

基金项目: 国家重大科技专项工程

作者简介: 李智勇(1975—), 男, 硕士学位, 高级工程师, 从事载人飞行器总体设计工作。联系电话: (010) 68746949。

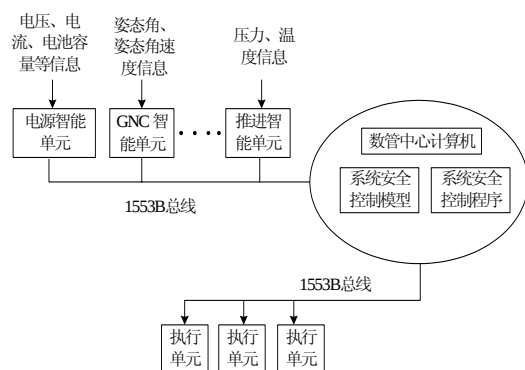


图1 载人飞行器自主控制原理框图

Fig. 1 Principle of autonomous control for manned spacecraft

2.1 能源系统安全性设计

根据故障模式影响分析(FMEA),有12种故障发生后果都是整器发电能力下降,电池放电深度逐渐增加直至超过允许值,最终导致飞行器因为能源不能平衡而失效。系统级能源安全设计主要针对此类故障开展。除了采用常规的熔断器、接地保护、配电单元相互隔离等负载端设计外,还针对供配电系统的故障后果进行自主安全设计。

若“天宫一号”在测控区内未及时处置故障或在测控区外发生的故障影响整器供电安全时,飞行器就进入能源安全模式,在保留平台设备开启的前提下,关闭部分供电负载,降低能源消耗,使蓄电池能够支持更长的时间为后续地面干预提供保障。能源安全管控由电源分系统和数管分系统共同完成。此项设计主要有两个难点,分别是控制参数的确定以及飞行器最小工作模型的确定。

2.1.1 电源控制参数的选择

在电流、电压、电池容量等参数中,电压和电流都是一种过程参数,往往需要通过全过程监测才能对故障进行判断,对于星载智能单元的判决要求较高。由于能源系统故障会导致电池容量降低,所以最终选取电池容量作为自主控制的判据:在电池容量消耗超过一定限度后,通过飞行器的数管计算机实施负载断电程序。

为避免毛刺干扰误触发安全模式,飞行器设置为连续多次电池容量超限才会进入安全处置程序;为确保判决参数的有效性,对电源分系统的

充放电控制软件进行了修改,以提取控制参数作为判据。

控制门限必须综合考虑载人飞行器的最小工作模型才能确定。

2.1.2 整器最小工作模型的确定

在“天宫一号”的不同飞行阶段,其最小工作模型是不同的。模型的建立有两个重点内容:一是配置,二是在这种配置下的最长工作时间。

配置主要由飞行器的功能决定。首先是自主飞行功能。在自主飞行期间,飞行器最小工作模型是指保证飞行器能源、测控、姿控和热控功能的最小配置。由于上述功能在实现时有耦合关系,比如热控所需的热量与加电工作的设备有关(如果设备关闭太多,就对飞行器内的热源产生影响,会影响热控功能的实现),在低功耗状态下存在电源系统的稳定性问题,所以在确定平台最小配置时必须综合考虑并进行必要的仿真分析。其次是交会对接功能。在交会过程中出现能源故障时,要考虑在平台最低配置基础上支持交会对接所需的测量、通信、对接设备的正常供电。第三是支持航天员驻留功能。有人交会对接时,需要考虑航天员生存所必需的供氧、供压、CO₂处理、湿度保持、照明和手动控制等载人环境控制设备的供电。统筹考虑上述3个方面条件才能确定能源安全模式下的最低配置,并根据各设备间的相互关系设置合理的关机程序。

最长工作时间是指从故障发生后到进入测控区工作的最长时间。假设最长工作时间是12h,那么必须考虑能源故障发生后,在12h内剩余能源能够支持飞行器继续工作,直到飞行器进入测控区后接受地面干预;否则方案不成立,必须修改最小配置。

2.1.3 电池容量安全门限的确定

根据最小配置和最长工作时间,可以计算出电池容量能否支持12h的飞行器能源消耗,并由此计算出自主飞行、交会对接阶段的电池放电深度。为避免误触发,安全门限值的设定既要比常规的放电深度大,又要保留足够的电容量以支持飞行器的后续故障处置。

“天宫一号”采用氢镍蓄电池组,充电控制

以 PT 控制为主。电池组容量通过对采集的每组电池的若干组温度、压力参数进行多数判决的方法计算得到,可靠性较高。因此正常情况下采用由 PT 计算得到的电池组容量作为故障判决参数,再由上述模型计算确定其安全门限。

2.1.4 能源安全模式的使用原则

载人飞行器能源安全模式的启动和关闭由地面观测的能源平衡状态来决策,通过地面的指令来进行切换。

受限于飞行器的起飞重量,所有的电子产品在重量设计上都有严格的限制。能源系统也不例外,这就限制了飞行器的发电、储电能力。根据能源平衡计算,飞行器的最大功耗发生在一些特定的工况中,这些工况的电池消耗将超过安全模式的触发值,因此必须对能源安全模式的使用加以限制,在某些设定的高功耗状态下关闭能源安全模式。根据测控覆盖性分析,这些工况期间的测控覆盖率能够达到 60%以上,可以快速注入降低负载的程序,手动干预进入安全模式。

2.1.5 负载关闭程序的实施

在“天宫一号”的设计中,使用 1553B 总线统一进行数据采集、指令分发的工作^[2]。数管计算机通过总线采集各智能单元的参数,当触发安全模式时,通过 1553B 总线发送程序预先设定的指令,将最低配置之外的设备在最短时间内陆续关闭。

地面根据遥测参数判别是否进入安全模式并开展后续处置。进入安全模式后,飞行器上的后续飞行程序都被删除。

能源安全性设计在飞行器测试中进行了验证:当设置的电池容量低于 50%时,触发了飞行器的保护程序,在 5 min 内,飞行器自主关闭了所有最小配置外的设备并保持了主要功能和性能稳定。

2.2 推进安全模式设计

为避免测控区外推进剂泄漏影响飞行器寿命,“天宫一号”设置了推进安全模式。推进安全模式设计旨在使飞行器对影响系统安全的重大故障(包括贮箱超压、发动机控制阀泄漏和气瓶泄

漏等)进行在轨自主检测、判断和处理,在出现故障后能够自主进入推进安全模式。

推进安全模式中自主故障检测与故障处理由推进分系统与数管分系统共同完成:推进智能单元完成传感器数据的采集以及故障的自动判别;通过 1553B 总线实现故障判别结果信息的传输;数管分系统根据结果信息发送对应的故障处理指令;推进执行单元根据指令执行故障处理。

2.3 III 象限天线自主接通模式

虽然中继卫星系统的建立大大扩大了测控覆盖范围,但是我国中继系统的应用是建立在飞行器中继天线能够准确指向中继卫星基础之上的,而精确指向需要飞行器姿态稳定——如果出现飞行器姿态失稳,中继通信将无法使用。

“天宫一号”在对地的 I 象限和对天的 III 象限均安装了宽波束测控天线,当双天线均接通时,能够形成准全向方向图。在长期在轨运行时,为增加对地发射功率,一般会断开 III 象限的天线。但是飞行器一旦姿态失稳且 I 象限不再对地时,地面的应急测控处置可能无法实现。为解决这个问题,“天宫一号”利用 GNC 分系统在姿态失稳时会自主进入对日定向模式的状态,由数管分系统连续多次判断处于“对日定向”状态时,即自主发送指令接通 III 象限天线,使飞行器能够顺利下传遥测数据并接收上行遥控信号。

3 经验和建议

“天宫一号”主要针对长期在轨运行自主管理,除了采取常规的分系统级热控、充放电、姿态控制等自主控制措施,还采用了系统级自主安全设计措施。系统级自主安全控制的主要特点是针对不同任务阶段和不同任务目标制定不同的工作模型以及相应的处置策略,以实现灵活的系统级自主控制。

“天宫一号”系统级自主安全设计除了能源系统自主安全控制外还考虑了其他自主控制模式,包括热控外回路自主控制、舱压自主控制等。这些自主控制模式都是选择表征飞行器关键功能的重要参数作为判决依据,合理制定判决门限和次数,利用飞行器的智能单元进行逻辑判断并进

行处置的,与图 1 的框架一致。

总结“天宫一号”系统级自主安全设计,有以下几点经验和建议:

1) 应当针对长期飞行特点和能源、测控等关键功能开展系统级自主安全设计,以确保平台的基本安全。

2) 系统级自主安全设计应当尽早开展。“天宫一号”系统级自主安全设计主要依托飞行器已有的设计资源开展工作,受产品既成状态约束,在模式选择、参数选择、准则设定、计算机性能等方面都无法进行太大的调整。系统级自主安全设计有待深入研究,例如能源安全模式应从发电各环节出发进行更有针对性的设计而不仅仅是降低负载功耗,推进安全模式的设计可以提前对推进分系统的软件功能提出要求等。

3) 系统级设计应当进行体系规划和功能设计。载人航天器自主安全模式设计是建立在各分系统已有自主功能基础上的一种应用,在开展设计时须针对各级智能单元的性能提出要求,确保

各种系统级安全设计得到自主实现。作为一个复杂系统,应当对安全模式有系统性的设计,从信息体系架构、计算机选型、分布式软件体系等方面开展顶层设计,才能更好地从系统层面保证飞行器的安全。

4 结束语

本文针对“天宫一号”目标飞行器长期在轨运行、短期有人照料的特点,以能源安全设计为主对其系统级自主安全设计进行了论述,总结了设计经验,对后续型号的设计提出了建议。

参考文献 (References)

- [1] 李尚福,黄席樾,魏洪波. 航天器发射飞行安全智能决策研究与实现[J]. 宇航学报, 2010, 31(3): 862-867
Li Shangfu, Huang Xiyue, Wei Hongbo. The realization of intelligent decision-making for space vehicle launching and safety controlling[J]. Journal of Astronautics, 2010, 31(3): 862-867
- [2] 徐洪平,闫俊武. 未来测量一体化设计构想[C]//第十二届全国遥测遥控技术年会, 2002

Design of systemic autonomous safety for Tiangong-I target spacecraft

Li Zhiyong

(Beijing Institute of Manned Space Systems Engineering, China Academy of Space Technology, Beijing 100094, China)

Abstract: In space flights, the safety of hardware during a long-time flight and that of astronaut during a short-time flight are important issues in the implementation of the mission goal. The capability of independent safety control should be designed for spacecraft in the system level against major faults beyond instant ground responses. This paper discusses the system design of autonomous safety for manned spacecraft, with primary concern on the power system. Some engineering practices and suggestions are summarized for further studies.

Key words: target spacecraft; flight safety; system design; power system