文章编号:1671-4598(2017)05-0029-03 DOI:10.16526/j.cnki.11—4762/tp.2017.05.009 中图分类号:TM93 文献标识码:A

基于拜占庭故障模式的空天飞行器GNC系统架构研究

石庆峰，梁 君，郎鹏飞，李 然，李艳美
（中国运载火箭技术研究院研究发展中心，北京 100076）

摘要：针对空天飞行器对GNC系统的高可靠性需求，开展了基于拜占庭故障模式的GNC系统架构研究，采用四机三总线架构设计方案，通过系统内总线实现输入数据及输出数据多机冗余比对，防止拜占庭故障的发生，提升了系统可靠性，实现了系统自检测和故障的准确定位及隔离，并具有在线故障诊断、故障自修复功能，同时解决了高动态、强干扰环境下系统自主性较差的问题，提升了GNC系统可靠性和容错性；经分析，该系统架构能够满足空天飞行器在轨、再入复杂任务需求。

关键词：空天飞行器；拜占庭故障；GNC系统；容错设计

GNC System Architecture Research for Aerospace Vehicle Based on Byzantine Failure mode

Shi Qingfeng，Liang Jun，Lang Pengfei，Li Ran，Li Yanmei
（R&D Center，China Academy of Launch Vehicle Technology，Beijing 100076，China）

Abstract：To meet the high reliability requirement of GNC system for aerospace vehicle (ASV)，developing the GNC system architecture research based on the Byzantine failure mode. This architecture is based on four computer processing modules and three MIL—1553B data buses，The comparison of the IO data through the system bus based on multi—computers redundancy. Byzantine fault is avoided，and the system reliability is improved. The GNC system has the function of fault detection，fault location，fault isolation and fault self—healing. The architecture solves the high dynamic and strong interference environment problems of the poor autonomy system. In addition，the system architechture can meet On—orbit and Reentry requirements.

Keywords：aerospace vehicle；Byzantine fault；GNC system；fault tolerance design

0 引言

空天飞行器是实现“快速、机动、廉价、可靠”进出空间的重要途径，具备可重复使用、长期在轨运行和快速应急响应等特点。是一个涉及多学科、多领域技术的大型复杂系统。飞行器在轨飞行和再入返回面临恶劣复杂的空间环境，加之我国在空天飞行器的研制方面还缺少充分的工程经验，且元器件、原材料和加工水平与国外还有一定差距，在轨段与再入段发生故障的可能性较大，美国航空航天局（NASA）哥达德空间飞行中心对1990年至2001年间全世界主要国家和地区发射的764颗航天器进行了故障统计，有35颗发生了GNC系统故障，而这35颗中有13颗全失效，占发生GNC系统故障航天器数的37 %[1]。GNC系统作为飞行器的核心控制系统，其可靠性直接影响着整个飞行任务的成败。美国在X—37B、“全球鹰”无人机等飞行器的控制系统上均采用了系统容错和重构技术；因此，为了确保飞行器可靠运行，必须提高GNC系统的可靠性，确保在故障发生后，能够及时检测故障和准确定位故障源，从而采取重构措施使故障影响降至最低，因此故障情况下的重构控制设计将大大提高任务成功的概率。

1 提高系统可靠性的手段

在航天器多余度系统设计方面，国际上有多种不同的方法和理论，应对的问题和情况也各不相同。空天飞行属于高性能、高可靠、高安全的任务，飞行器有较强的资源限制条件，因此在多余度体系结构和系统详细设计方面应综合考虑各方因素。提高系统可靠性目前主要有两种措施，一是“避错”设计，即在方案设计阶段就要保证系统无缺陷、无故障发生，该方法实际上是要求系统完美无暇，不能出现绝对的差错，从系统研制的角度来看该设计理念是一种理想行为，按照该方法不仅系统研制代价巨大，而且系统出故障概率为零也不现实。再一种设计方法就是“容错”设计，顾名思义就是即使系统出现故障，但因自身具备强大的容错能力，也能保证系统功能不受影响。可见系统容错设计是航天器应对故障问题最有效的措施。

在系统级故障容错方面，由于空天飞行器需要进行高超声速大气层返回再入和机场着陆任务，因此要求GNC系统在多重故障情况下仍然可以正常连续工作，以保证飞行器关键任务安全。在系统级自动重构方面，目前国际上有几种典型的系统重构策略，如美国喷气推进实验室研制成功的STAR容错计算机，通过采用冗余技术，其可靠性比单一计算机高几十倍，可以对系统出现的各种瞬时、永久、随机和灾难性的故障实现容错。如国际空间站主要应对长期在轨和有人值守的飞行任务情况，优先保证系统长期工作可靠性，并可以通过人工维修和更换使系统二次重构，恢复系统因偶然故障失去的可靠性冗余；X—37主要考虑高速再入时系统的快速重构能力，保证系统在发生故障时可以无缝切换为新的构型，并保证飞行任务安全。

在国内，提高飞行器可靠性的主要手段大多基于“三取二表决机制”。即GNC系统采用三冗余设计方案，该方案虽然

收稿日期：2016-10-26； 修回日期：2016-12-15。

作者简介：石庆峰(1975-)，男，山东临沂人，硕士研究生，高级工程师，主要从事导航、制导与控制方向的研究。

在一定程度上达到了容错目的，但该容错机制在系统出现两度故障后将失效，系统容错能力不足。对于空天飞行器来说，高动态连续工作和长期在轨都要求系统具有很高的可靠性，且具备应对多重故障的能力，为了保证系统在两度故障模式下还仍具备容错能力，容错方案设计中必须考虑拜占庭故障模式。根据文献[2]的证明，若要解决一重拜占庭故障，则需要至少 4 个计算机同时工作。

2 拜占庭故障模式简介

拜占庭问题的最初描述是：n 个将军被分隔在不同地方，忠诚的将军希望通过某种协议达成某个命令的一致，但其中一些背叛的将军会通过发送错误的消息阻挠忠诚的将军达成命令上的一致，拜占庭问题就此形成。美国计算机学家莱斯利·兰伯特（Leslie Lamport）[3]证明了在将军总数大于 $3n$，背叛者为 n 个或更少时，忠诚的将军可以达成命令上的一致。

从工程的角度来说，一个可靠的系统必须能够应对多重故障模式，发生故障的部件可能会向系统中不同的对象发送相互矛盾的信息，该类故障便可以抽象为拜占庭将军问题。在三模冗余系统中，拜占庭将军问题可简化为图 1。

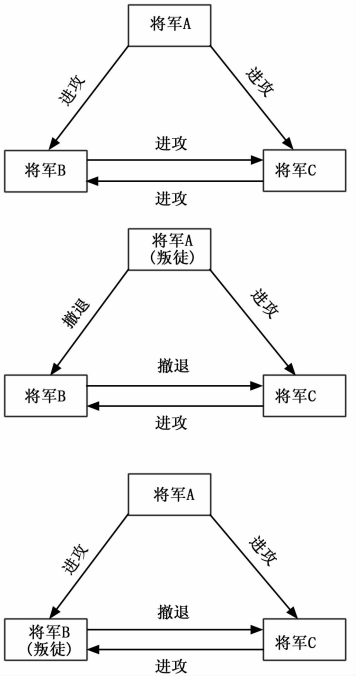

图 1 三模冗余模式下的拜占庭问题

3 空天飞行器 GNC 系统架构设计

3.1 总体设计思路

（1）采用四机冗余及容错设计，以最少部件实现最大冗余，以最少接口实现全周期 GNC 功能，增强接口匹配能力，减少接口之间的测试、协调；

（2）通过系统内总线实现输入数据及输出数据多机冗余比对，防止拜占庭故障的发生，提升系统可靠性，当某一模块故障后，能够实现自主检测、准确定位。

3.2 系统方案设计

3.2.1 架构设计

空天飞行器 GNC 系统采用四机三总线架构，四个控制模块和三条总线的结构实现了飞行器安全和高可靠运行。三条 1553B 总线，完成导航信息及控制指令的传输，实现飞控计算机与敏感器及执行机构的信息交互；采用四机冗余的飞控计算机进行全系统导航信息处理及制导控制指令的发出；采用双冗余或三冗余敏感器完成航天器全任务段信息采集；采用三冗余执行机构来执行飞控计算机发出的控制指令，架构设计示意图如图 2 所示。

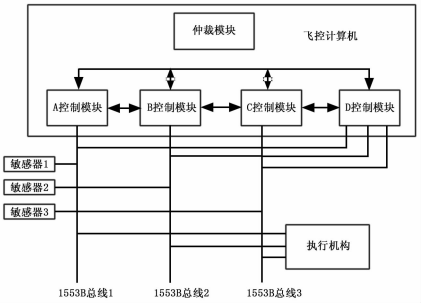

图 2 空天飞行器 GNC 系统架构示意图

飞控计算机包括 A、B、C、D 四个相同的控制模块（即四备份冗余设计）和仲裁模块；飞控计算机的 A、B 和 C 三个控制模块分别作为 BC（总线控制器）管理 GNC 系统的三条 1553B 总线，D 计算机处于温备份状态。A、B 和 C 三个控制模块中的任意一个模块出现故障，D 控制模块能够替代故障控制模块作为 BC 管理故障模块管理的 1553B 总线。

3.2.2 容错设计

飞控计算机的 A、B 和 C 三个控制模块分别接收通过对应 1553B 总线传输的敏感器信息，D 控制模块接收三条 1553B 总线传输的所有数据，A、B、C 和 D 控制模块将各自接收到的 1553B 总线传输的数据进行两两之间的信息交互，并将各自接收到的数据发送至仲裁模块（该模块对 A、B、C 和 D 控制模块进行仲裁，不接收输入信息，也不输出指令，避免外接口对模块的干扰，可靠性更高）；A、B、C、D 四个控制模块和仲裁模块分别将交互后各自包含的系统信息进行处理，得到飞行器的实时位置、姿态、轨道信息，并各自结合执行机构状态计算出控制指令，然后将各自形成的控制指令进行两两之间的指令交互，各控制模块将交互完后包含的指令进行表决并通过 1553B 总线输出最终的控制指令给执行机构；同时通过指令表决的方式判断是否存在故障模块，并将故障模块进行隔离。数据交互比对具体说明如下：

（1）输入比对：各模块分别接收 GNC 系统 1553B 总线上的数据，把 1553B 总线数据转换成飞控计算机内总线数据，通过内总线传递给仲裁模块进行输入数据交换；

（2）输出比对：飞控计算机各模块通过内总线接收仲裁模块经过表决的输出数据，并转化成 GNC 系统 1553B 总线数据，经 1553B 总线输出。

当四冗余飞控计算机中某一模块同其它模块不能同步，或虽能同步但连续多次表决数据不正确以及软件看门狗溢出，则认为该控制模块发生了严重故障，就要进行系统重试，对故障模块进行重构。重试时，三个正常控制模块先将故障模块从系统中切除，使系统降模为三模工作方式，然后将故障控制模块复位或是再加电。

下面以一个具体例子说明飞控计算机内 A、B、C、D 四个控制模块进行指令交互、表决和判断故障模块的具体实现方式：

假设将飞控计算机 A、B、C 控制模块分别作为 1553B 总

线 1、总线 2、总线 3 的 BC，将备份的 D 控制模块挂在三条总线上（能够管理 1553B 总线 1、总线 2、总线 3）。

（1）数据交换。

各控制模块和仲裁模块将各自形成的控制指令进行两两之间的指令交互，使得每个控制模块都会生成一个信息矩阵。举例说明：

假定飞控计算机 A 控制模块发送数据 1，B 控制模块发送数据 2，C 控制模块发送数据 3，D 控制模块发送数据 4，而 B 控制模块出现故障。各控制模块发送自己的数据给对方，也同时发给仲裁模块。其中 A、C、D 控制模块发送的是其真实值，而 B 控制模块可能对其他机发送不同的信息。则在第 1 轮数据交换后每个控制模块和仲裁模块都会有 1 个所有控制模块的信息，即：

A 控制模块［1，a，3，4］，B 控制模块［1，2，3，4］，C 控制模块［1，b，3，4］，D 控制模块［1，c，3，4］，仲裁模块［1，d，3，4］。

各控制模块将自己接收到的数据再向其他控制模块转发，这样每个控制模块都会生成一个信息矩阵，即：

$$A\text{ 模块}\begin{bmatrix}1 & a & 3 & 4\\ e & f & g & h\\ 1 & b & 3 & 4\\ 1 & c & 3 & 4\\ 1 & d & 3 & 4\end{bmatrix},B\text{ 模块}\begin{bmatrix}1 & a & 3 & 4\\ 1 & 2 & 3 & 4\\ 1 & b & 3 & 4\\ 1 & c & 3 & 4\\ 1 & d & 3 & 4\end{bmatrix},$$

$$C\text{ 模块}\begin{bmatrix}1 & a & 3 & 4\\ m & n & p & q\\ 1 & b & 3 & 4\\ 1 & c & 3 & 4\\ 1 & d & 3 & 4\end{bmatrix},D\text{ 模块}\begin{bmatrix}1 & a & 3 & 4\\ r & s & t & u\\ 1 & b & 3 & 4\\ 1 & c & 3 & 4\\ 1 & d & 3 & 4\end{bmatrix},$$

$$\text{仲裁模块}\begin{bmatrix}1 & a & 3 & 4\\ v & w & x & y\\ 1 & b & 3 & 4\\ 1 & c & 3 & 4\\ 1 & d & 3 & 4\end{bmatrix}$$

其中：a、b、c、d、e、f、g、h、r、s、t、u、v、w、x、y 是 B 模块向其他模块发送的错误数据；以 A 模块为例，第一行［1，a，3，4］是 1 轮数据交换后 A 模块的数据，第一行的 a 是 B 模块发送的，其余分别对应着 A 模块自己的数和 C、D 模块的发送的数据；第二轮数据交换是各模块将各自拥有的数据发送给对方，［e、f、g、h］是 B 模块发送的（因为 B 模块发送的是错误数据，所以四个数全部是错误的）；［1、b、3、4］、［1、c、3、4］、［1、d、3、4］分别是 C、D 和仲裁模块发送的；

（2）指令表决。

各控制模块和仲裁模块按照少数服从多数的原则进行表决，对信息矩阵的每一列进行选择，如果在某一列中的某个指令的数量大于等于三个（在表决第 i 列时，应将对应第 i 行数除外，该行数为自身的数据），则该指令为表决输出的正确指令；如果某一列中不存在数量大于三个的指令，则认为该控制模块故障，同时如果某一列中的指令的数量小于三个，则与其对应的控制模块故障；

在上述例程中，通过表决得到结果如下：

A 模块：（1，UNKOWN，3，4）；C 模块：（1，UNKOWN，3，4）；D 模块：（1，UNKOWN，3，4）；仲裁模块：（1，UNKOWN，3，4）。

A、C、D 三机和仲裁模块一致认为 B 机发生故障，在表决 B 机的数据时，虽然没有某个数占多数，但各机中参与表决的 4 个数是一样的，都是（a，b，c，d），那么各机表决结果也必定是一致的。至此，检测出 B 机出现故障，并将其隔离。

（3）将步骤（2）判定故障的 B 控制模块进行隔离。

3.2.3　同步策略

飞控计算机每个控制模块都产生一个用于本地的软时钟信号，时钟周期可根据具体控制方案确定。软时钟可通过模块中的 FPGA 实现，并根据实际需求确定同步脉冲的占空比。

每个控制模块在被复位后，都会向其他三个模块发送一个“复位准备好标识”，表示本模块已处于复位后待命状态。当每个模块通过 FPGA 读取到其它三个模块的“复位准备好标识”后，便开始启动运行。这样便实现了四模块的起始同步。

由于每个模块的软时钟都是基于本地钟振产生，而每个钟振之间又存在偏差，所以随着时间的推移，通过 FPGA 计数器产生的软时钟之间的偏差就会越来越大，为了阻止这种偏差扩大，将其控制在一个可容忍的范围之内，就要定期对四个模块的软时钟进行同步。软时钟同步的主要内容有三项：首先获得其他机器软时钟信息，然后根据这些信息计算得出本地时钟与其他模块软时钟之间的偏差，最后用所获得的偏差对本地软时钟进行修正。

3.2.4　突破的关键技术

采用基于拜占庭故障模式的系统架构降低了飞行器进出空间过程中大过载、高速、高动态环境下 GNC 系统面临的风险。突破了多余度快速自动重构关键技术。基于关键技术建立的多余度、变结构 GNC 系统体系结构可以满足系统全任务期间系统容错使用需求，且系统在任意一重故障下能够正常工作，在二重故障下保飞行任务安全；系统自动重构所需时间不大于一个系统控制周期；此外，系统具备自动故障恢复功能，长时间在轨运行可靠性不受偶发故障累积影响。通过对基于拜占庭故障模式的 GNC 系统架构进行仿真验证，结果满足可靠性要求。具体结果见表 1。

表 1　控制器单机故障仿真及重构验证结果

序号	故障模式	时间坐标		验证结果
		造成影响	容错/重构方案	
1.	控制器 A 机故障	A 机完全失效	由 D 机代替 A 的任务继续运行	正常
2.	控制器 B 机故障	B 机完全失效	由 D 机代替 B 的任务继续运行	正常
3.	控制器 C 机故障	C 机完全失效	由 D 机代替 C 的任务继续运行	正常
4.	控制器 D 机故障	D 机完全失效	A/B/C 机按之前的模式继续运行	正常

4　结束语

基于拜占庭故障模式的架构设计技术是改善空天飞行器 GNC 系统可靠性的有效手段，基于该技术设计的系统具备高可靠性、多冗余自动重构能力，是发展“高精度、高可靠性、

（下转第 55 页）

②传感器距离如果管路上有弯头、变径、阀门和泵等，要保证一定的距离，因为在弯头、变径、阀门和泵的附近容易产生涡流，影响测量数据，具体距离参数可查找安装说明的参数表，传感器一般与之都要相距 10 倍管径以上；

③如果选择垂直地面的管路测量，要注意液体的流向，要选择液体向上流动的管路，因为液体向下流动时，受重力的影响，容易造成液柱不连续，有气泡产生，影响测量精度。

5　二次仪表的使用及数据采集

超声波流量计的探头通过同轴电缆与二次仪表相连，二次仪表通过采集超声波信号，进行相关计算，得到流量值。

二次仪表需要输入输油管路的管径参数，超声波在煤油中的传播速度，煤油密度、黏度系数、测试电缆长度等参数[6]。

测量仪表计算出流量值后，可以根据设定的量程范围变送输出标准的电流电压信号，供计算机测试系统采集记录。

6　超声波流量计的在飞机燃油试验中具体应用

在飞机燃油试验中需要采用油箱标定的方法来测量输油流量。在以往的型号试验中油箱标定的方法是通过逐次向油箱内加入一定量的煤油，记录下油箱内液位传感器的液位高度，得到油箱的油量－高度曲线。在油箱标定试验中，油箱输油，记录下油箱内液位传感器的液位高度变化，通过油量－高度曲线计算得到油箱油量随时间变化曲线，其斜率是油箱输油瞬时流量。但是油箱标定是一项很庞大的试验，虽然试验本身并不复杂，但需要耗费大量人力物力，在某型飞机油量标定试验中，整个试验团队用两个月才完成标定试验。并且在飞机燃油试验中，试验需要测试不同油箱在不同姿态下的输油流量，而涡轮流量计的体积很大，不适合安装在油箱内的狭小空间，因此不能安装涡轮流量计，为了保住试验节点不能再使用的耗时耗力的测量方法。所以，需要采用一种新的技术或测量方法来完成油箱输油流量的测量。经过调研论证，发现了一种新型流量测量仪器—超声波流量计进行流量测量。超声波流量计的优点是体积很小、适合安装在输油管路的外管壁上，不会破坏输油管路流阻特性，并且其防爆等级是二区防爆 ExdII BT4 符合飞机燃油试验要求，可以浸泡在油箱煤油中测量油箱内部管路的煤油流量。

团队首次将超声波流量计应用到飞机燃油试验中，而其中最大亮点就是首次使用超声波流量计测量浸在飞机油箱中的输油管路的输油流量。

下面结合测量机翼油箱的输油流量测量介绍超声波流量计的在飞机燃油试验中具体应用。

首先打开油箱口盖，确认需要测量的管路，选择测量位置时要参照上文所述的安装位置选择注意事项。

通过查阅管路设计图纸，获得待测输油管路的材料型号、管径、壁厚等参数指标，经确认，机翼油箱的输油管路材料为铝、外径（XX）mm、壁厚（XX）mm，将这些参数输入测量仪表，测量仪表经过内部计算，给出最优的安装方式和探头之间的最佳间距。

在确定好安装位置后，按照测量仪表提示的安装方式和间距进行安装，安装时一定要注意探头的中心线与管路轴线平行，参照前文论述，另外注意探头的方向与管路中煤油流向一致。

探头固定好后，用千分卡尺测量两个探头之间的实际距离，虽然安装时是尽量按照仪表给出的尺寸安装，但由于安装空间限制，实际距离与要求距离不能完全相同，但只要将实际距离输入测量仪表，测量仪表根据实际距离进行修正。

探头固定安装后，将探头的测试电缆与测量仪表连接，这时，如果管路中充满煤油，仪表的测试界面将显示超声波信号强弱，如果信号很强，则表明探头安装正确，如果信号弱，则需检查探头安装情况，调整安装，直至显示信号正常，可以进行试验测试。

测试仪表将测得的流量值输入给计算机测试系统，计算机系统同步记录流量值和试验中其他参数，从而完成输油流量测量试验。

7　结论

本文介绍了超声波流量计在飞机燃油试验中的实际应用，并且在近期几个型号的燃油地面模拟试验中，都应用了超声波流量计测量输油流量，由于其安装测试简单方便，节省大量的人力物力，解决了费时费力的测试难题，很好地完成试验任务，确保了试验节点。综上，在飞机燃油流量测试中应用超声波流量计是可行的，并且本方法已经在飞机燃油模拟试验的流量测试中得到成功运用。建议该测试方法在飞机其他系统流量测试中使用，比如液压系统、环控系统都非常适合使用该方法。同时，该测试方法在飞机机上排故方面会起重大作用。随着超声波流量计发展，测试设备越来越小，并且可以应用在机上燃油流量测试。

参考文献：

[1] 罗伊·兰顿. 飞机燃油系统［M］. 上海：上海交通大学出版社，2010.

[2] 黄挚雄. 超声波流量计的发展与应用［J］. 自动化与仪表，1998(3)：1－4.

[3] 陈　聪. 超声波流量计的特点和应用［J］. 医药工程技术，2010(1)：48－50.

[4] 刘　杰. 基于时差法的超声波流量计设计［D］. 哈尔滨：哈尔滨工程大学，2010.

[5] 王立琦，王　珍. 高精度超声波流量计的研制［J］. 哈尔滨商业大学学报，2001.

[6] 兰纯纯. 时差式超声波流量计二次仪表的研究［D］. 杭州：浙江大学机械能源学院，2004.

（上接第 31 页）

长寿命”GNC 系统的关键技术之一。能够满足空天飞行器在轨、再入复杂环境下的任务要求，该设计理念可为后续同类航天器的设计提供参考 。

参考文献：

[1] 林来兴，最近十年航天器制导、导航与控制（GNC ）系统故障分析研究［J］. 控制工程，2004，(1)：1－2.

[2] K PKihlstrom，L E Moser，P M Melliar－Smith. Solving Consen－sus in a Byzantine Environment Using an Unreliable Fault Detector［A］. Proceedings of the International Conference on Principles of Distributed Systems（OPODIS）［C］. 1997.

[3] Leslie Lamport，Robert Shostak，Marshall Pease. The byzantine generals problem［J］. ACM Transactions on Programming Language and Systems，1982，4（3）：382－401.