运载火箭故障检测处理系统软件研究和实践

贺　菲
（北京宇航系统工程研究所）

摘　要　介绍载人运载火箭故障检测处理系统软件的主要情况、重要故障模式和特点，从软件研制过程、配置管理、技术状态控制、软件测试、可靠性安全性等方面总结了故障检测处理系统软件工程化的经验，为下一步任务提供参考与借鉴。

关键词　运载火箭　故障检测处理系统　软件工程化

1 前言

载人运载火箭是为载人航天工程研制的，具有高可靠性、高安全性特点。为了保障航天员在上升段的生命安全，建立故障检测处理系统（以下简称故检系统）。

故检系统的主要任务是在临射前 30 分钟开始到上升段船箭分离这段时间内，检测运载火箭的重要参数，判断运载火箭的飞行状态是否正常，将检测的结果实时通知航天员，并在运载火箭出现故障的情况下，根据不同的逃逸模式实施逃逸。

故检系统软件包括两部分，箭上飞行控制软件和地面测发控软件，分别实现运载火箭重要参数检测、故障判断、实施逃逸和地面测发控。故检系统软件直接影响到运载火箭飞行的成败和航天员的生命安全。

2 故检系统软件简介

2.1 箭上飞行软件

故检系统箭上飞行软件分成故障检测处理和逃逸程序控制两部分，分别运行在故障检测处理器和逃逸程序控制器上。

故障检测处理软件从运载火箭起飞前 30min 开始运行到船箭正常分离为止。其主要功能是巡检运载火箭的重要参数，根据故障判别模式，对这些参数进行数据处理并输出判别结果。

逃逸程序控制软件从运载火箭起飞前 30min 开始运行到整流罩分离，逃逸程序控制器随之抛离为止。其主要功能是执行具体的逃逸时序动作。

两个箭上软件内部有一单工串行通讯接口，故障检测处理软件通过此接口向逃逸程序控制软件发送逃逸参数。

2.2 地面测发控软件

在运载火箭进入基地技术阵地，到运载火箭成功发射这一段时间内，地面测发控软件通过后端微机对前端地面设备的控制，完成对箭上设备箭上飞行软件装订，测试数据的实时采集、存储、显示，事后处理及打印，并完成系统射前的测发控功能。

3 重要故障模式

3.1 开关量故障判断模式

表 1　分离量信号判断模式

开关量名	代号	报警上限代号	报警下限代号
逃逸塔分离信号	T1	$T1^-$	$T1^+$
助推器 1~4 分离信号	T2	$T2^-$	$T2^+$
一、二级分离信号	T3	$T3^-$	$T3^+$
整流罩横纵分离信号	T4	$T4^-$	$T4^+$
二级副系统关机	T5	$T5^-$	$T5^+$

在报警上限之前收到分离信号或在报警下限之后收到分离信号均输出报警信号。

其中：助推器分离信号的具体判断准则为：

在飞行时间 $T<T2^-$ 时，有 1 或 1 个以上的助推器分离时，输出报警信号；

在飞行时间 T>T2*时，小于 3 个助推器分离时，输出报警信号；

其它情况正常。

3.2 模拟量故障判断模式

3.2.1 轴向过载

由于轴向过载 NX 在飞行中为一条曲线，所以在软件中依据此曲线以整秒存入一个理论数据表。对于非整时间所对应的 NX 值，利用图 1 的插值法求得。

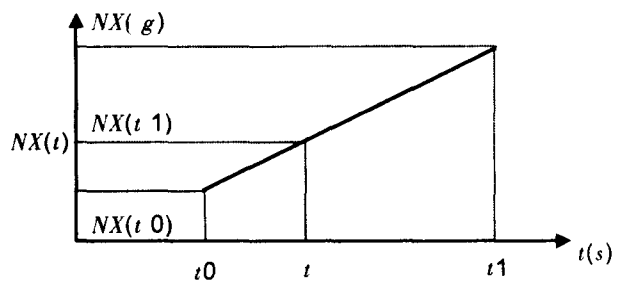

图 1 NX 插值计算

当故障检测处理器获得一个 t 时刻的轴向过载 $NX(t)$后做如下处理：

如果 $t_i \leqslant t \leqslant t_{i+1}(i \in N)$，当 i 足够大时，用线性插值计算 $NX_{gz}(t)=\frac{t-t_i}{t_{i+1}-t_i}[NX_{gz}(t_{i+1})-NX_{gz}(t_i)]+NX_{gz}(t_i)$

若 $NX(t) \leqslant NX_{gz}(t)$，则输出逃逸指令。

3.2.2 姿态角偏差

在船箭分离前的飞行时间段内，当首次检测到箭体的平台姿态角超出报警限，发出报警信号；当检测到箭体的平台姿态角超出故障限，在无切换信号时判断捷联角速率积分增量和平台姿态角增量的一致性；若同一个量的两个增量结果一致、时间大于 DTQ（姿态角超限且未收到切换信号时的等待时间）且连续多次同时满足判定故障的条件，则发出故障信号和逃逸指令。若同一个量的两个增量结果不一致，时间超过 DTQ 后，捷联角速率积分增量超故障限，上述条件连续多次同时满足则发出故障信号和逃逸指令。

当故检系统接到平台切换信号后，不再进行平台姿态角偏差、捷联角速率参数的采集处理和判断。故检系统用箭体俯仰角速率和偏航角速率的积分增量来判断姿态故障。

3.2.3 箭体角速率

箭体角速率用于姿态故障判断时，首先要将角速率处理成给定时间内的积分增量，然后进行姿态故障的判断。其判断方法是：确认收到平台切换信号后，当同一通道的两路信号的积分增量连续超过故障限且一致时，发出报警信号、故障信号和逃逸指令。箭体角速率积分增量的处理方法同 3.2.4。

3.2.4 捷联惯组角速率积分增量

故检系统首先将捷联惯组角速率模拟量电压值转成姿态角。数据转换方法如下：

$\omega x(\omega y,\omega z)=k0+k1\mathrm{Ui}$，系数 $k0$、$k1$ 是传感器联校系数。

在确定物理量之后，再将它们处理成 DT 时间内的增量，在时刻 t 的捷联俯仰角速率积分增量为：

$$\Delta\varphi_{inc}^{J}=\int_{t'}^{t}\omega_z\,dt-\Delta\varphi_{cx}=\sum_{i=1}^{n}0.5(\omega_z^{i}+\omega_z^{i-1})\Delta t-(\varphi_{cx}^{n}-\varphi_{cx}^{0})$$

其中 $t-t'$=DT，Δt 为积分步长，$(\varphi_{cx}^{n}-\varphi_{cx}^{0})$ 是程序角 DT 时间内的增量。

在时刻 t 的捷联偏航角速率和捷联滚动角速率积分增量为：

$$\Delta\psi(\gamma)_{inc}^{J}=\int_{t'}^{t}\omega_z(\omega_z)dt=\sum_{i=1}^{n}0.5\left[\omega_y(\omega_x)^{i}+\omega_y(\omega_x)^{i-1}\right]\Delta t$$

其中 $t-t'$=DT，Δt 为积分步长。

在平台切换前，捷联角速率积分增量同平台姿态角增量一起判断姿态故障。

4 故检系统软件的特点

故检系统软件产品包括箭上软件和地面软件累计 20 个，且软件的规模差异性大。故检系统软件规模情况见表 2。

表 2 故检系统软件规模情况

序号	软件规模定义	故检系统软件各规模数量	占故检软件总数百分比
1	大(10000≤代码行数<100000)	1	5%
2	中(3000≤代码行数<10000)	2	10%
3	小(300≤代码行数<3000)	12	60%
4	微(代码行数<300)	5	25%

故检系统软件的成败直接影响运载火箭飞行的成败和航天员的生命安全。因此，其具有高可靠性和高安全性。故检系统软件关键等级情况见表 3。

表 3 故检系统软件关键等级情况

序号	软件关键等级	故检软件各等级数量	占故检软件总数百分比
1	A	2	10%
2	B	4	20%
3	C	9	45%
4	D	5	25%

故障判据的变化将引起故检系统箭上飞行软件的变化。遥四箭~遥七箭故检系统软件更改情况见图 2。

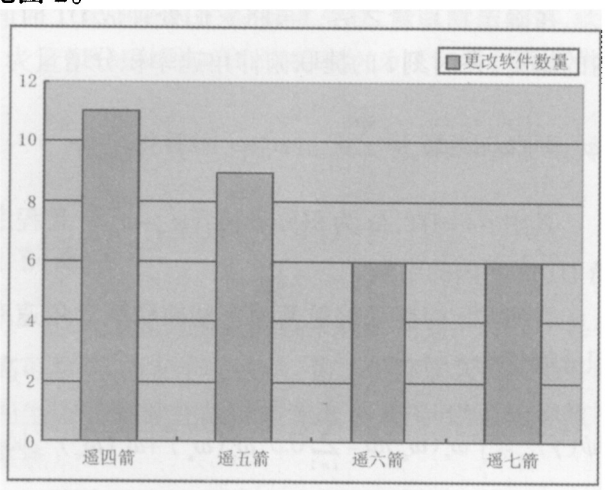

图 2 故检系统软件更改情况

故检系统软件接口复杂。包括系统内部软件接口、与运载火箭其他电气系统软件接口、与飞船系统软件接口。

5 故检系统软件工程化实践

5.1 研制过程

结合故检系统软件的特点和软件工程化的要求，对故检系统软件产品的研制开发和管理分阶段进行，明确规范了故检系统软件产品的研制技术流程，见图 3。

该流程要点如下：

·对有更改的软件制定全过程研制流程，对每个研制阶段都设置检查点进行严格控制，确保软件研制过程受控；

·沿用软件的研制技术流程，重点放在对软件的需求分析、设计、实现、测试等环节的清理和复核，经过系统综合试验进行考核，保证沿用软件的正确性；

·全箭系统级试验的流程主要验证各系统接口的匹配性。

5.2 文档编制

通过规范故检系统软件文档的编制，推动故检系统软件工程化工作。

·按照软件开发过程编制文档，做到文档齐全、文文一致；

·每次飞行任务故检系统软件均形成独立、齐全的文档，所有文档都纳入软件配置管理；

·故检系统软件开发阶段的文档严格按照规范的要求编写；

·在软件研制过程中设置检查点，组织软件专家对文档进行检查，并及时修正文档；

·要求第三方协助进行软件文档的齐全性、正确性和文文一致性审查。

5.3 可靠性、安全性

故检系统软件直接关系到航天员的生命安全，因此，对其可靠性和安全性有很高的要求。为了确保

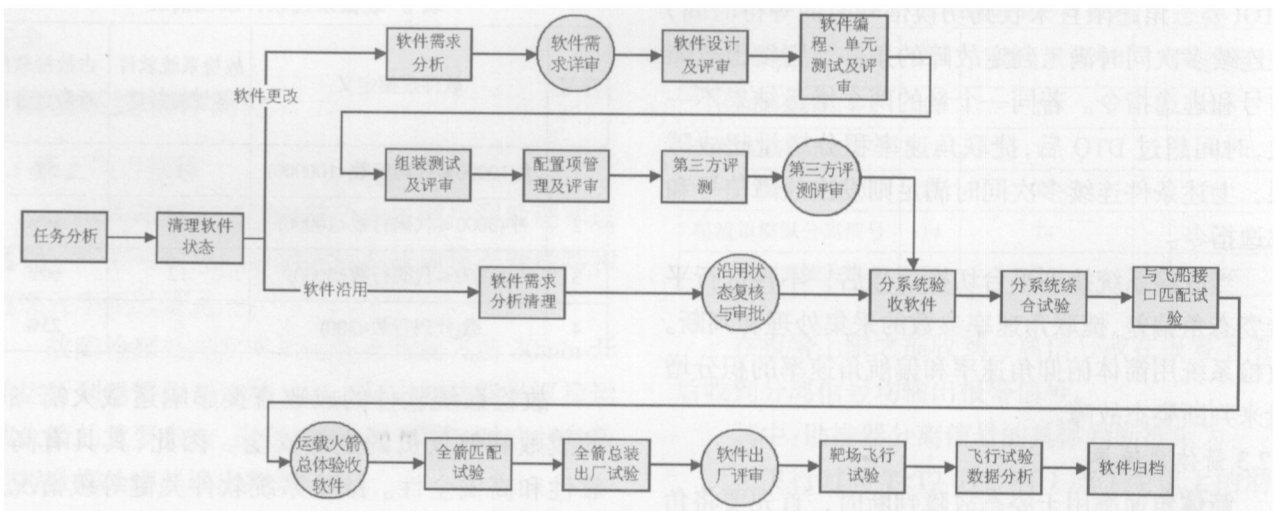

图 3 故检系统软件研制流程

故检系统软件的可靠性和安全性，我们从可靠性和安全性设计、分析和测试等方面开展工作。

5.3.1 可靠性、安全设计

· 所有的输入信号都做了以一定时间间隔的多次采集，然后再进行判断，以避免干扰信号影响故障判断的准确性。所有中断触发的功能在响应中断后还要对触发信号进行确认，以免误动作；

· 所有报警限和故障限数据采用冗余备份，使用时求冗余数据的中间值，确保报警限和故障限的准确和可靠；

· 软件中重要的变量都有冗余，做 N/P(G)判定后才使用；

· 避免使用位判断，而是将位信息转化为字节信息，避免了因某一位跳变而引起误判；

· 不用全 0 或全 1 表示逻辑零或逻辑一，而是用有特定意义的十六进制数据来表示；

· 逃逸参数直接关系到控制发动机的正确动作。因此，同时发送多组逃逸参数，接收端进行 N/P(G)判定，并判断其合理性后才使用；

· 为提高故障判断的准确率和可靠性，使用连续多次参数的巡检和判定的方法来确定是否故障；

· 对开关量的各信号位做 N/P(G)判定。

· 对重要功能均有冗余设计。如供电、发射控制功能为主、副两套独立系统互为备份；向箭上装订程序是前、后端互为备份等等。

· 采用 CRC 校验增强串行通讯的可靠性；

· 每次代码发送完毕后都要进行代码回传并加以比较，确认无误后才启动箭上程序，以确保向箭上装订程序的可靠性；

· 为防止起飞和紧急关机中断恢复现场时恢复起飞前的故障而引起逃逸，在关键时间段清除故障和报警；

· 在屏蔽逃逸区内无手动逃逸时清除故障输出；

· 在除零保护、边界处理、数据转换等方面采取了容错设计。

5.3.2 可靠性、安全性测试

在功能、性能测试逐步完善的基础上，对故检系统软件开展了边界测试、余量测试、强度测试等方面的工作。

· 边界测试主要是测试软件在系统输入域（或输出域）、状态转换、功能界限、性能界限、容量界限等的边界情况下软件运行状态是否正常；

· 余量测试主要测试软件的存储量、输入及通道等资源，以及功能处理时间的余量是否满足设计要求；

· 强度测试进行性能和降级能力的强度测试。前者是在测试过程某些阶段，软件在饱和态下运行，测试软件的响应时间、数据处理能力等；后者是对设计上允许降级运行的计算机系统的每种可能降级方式进行测试验证。

5.4 配置管理

为控制故检系统软件产品的质量，保证软件状态受控，故检系统软件共设置了 20 个软件配置项，建立了软件开发库、受控库和产品库，由专门的软件配置管理员负责配置管理工作。按照软件任务书进行软件编制时，软件状态由开发库管理控制；单元测试通过后，软件提交软件状态受控库，由软件状态受控库提取软件交第三方进行确认测试；第三方确认测试通过后的软件提交软件产品库，系统测试和飞行试验使用的软件由软件产品库中提取。

5.4.1 制定软件配置管理要求，明确以下内容

· 软件开发库、受控库和产品库中所管理的软件清单；

· 保证软件正确性、完备性、一致性和可追踪性的具体措施；

· 入库、出库的控制办法和审批手续；

· 软件更改控制的办法和审批手续。

5.4.2 对更改软件出/入库配置进行严格控制

· 软件工程师更改软件版本、交付第三方评测和交付产品库存档的软件均从受控库中提取，并填写《软件受控库出库申请单》；

· 受控库软件的更改都要填写《软件问题报告单》、《软件更改报告单》、《软件更改入库申请单》，软件工程师将更改后的软件入受控库时，将此三单一并入库。

5.4.3 对沿用软件的配置和版本进行严格控制

· 经沿用确认的软件产品存入软件产品库；

· 按要求整理、配套沿用软件的文档；

· 从产品库中提取沿用软件，并参加系统综合试验。

5.4.4 严格控制软件出/入产品库

· 软件出/入产品库都要填写《软件出/入产品库

申请单》,并经三级审批;

· 软件出/入产品库都要填写《软件产品证明书》和《软件质量履历书》,随软件产品流动,作为原始记录备查。

5.5 技术状态控制

故检系统软件产品同硬件产品一样严格进行技术状态控制，对每项技术状态变化都严格做到论证充分、各方认可、试验验证、审批完备、落实到位。对技术状态不变的软件产品采用能够沿用复核确认的方式进行控制。故检系统软件技术状态管理和控制有以下特点:

5.5.1 严格管理故检系统软件的技术状态更改,实现闭环控制

· 由总体提出的需求变化报总师批准，以技术文件的形式下发系统执行;

· 对总体要求进行更改的项目，系统必须进行影响分析和相应的试验验证,并形成报告反馈给总体;

· 对系统进一步提高可靠性、安全性设计等原因而提出的更改,必须按技术状态变化"五条"标准进行,并办理"技术状态更改申请单";

· 更改后的软件,必须进行软件版本升级,并进行回归测试、系统综合试验、全箭匹配试验、全箭出厂试验验证。通过各项测试和试验验证后,办理"技术状态更改落实单",完成闭环控制。

5.5.2 复核技术状态不变的软件是否满足沿用的条件。复核工作包括一下方面:

· 分析软件任务需求是否有变化;

· 分析软件运行环境是否有变化;

· 复查软件经历的测试和飞行试验考核情况;

· 复查软件配置管理情况。

5.6 软件测试

进行全面、有效的软件测试是保证软件质量的重要手段。我们的软件工程师对故检系统软件进行了详细的静态测试和单元测试。另外,按照总装和集团公司的要求，我们对故检系统软件做了严格的独立第三方测试。发现软件问题后,必须在有软件问题报告单的前提下方可修改,并有相应的修改记录。对改正的软件进行回归测试，通过回归测试的软件再入软件产品库。严格细致的测试工作确保了软件的质量。

故检系统软件的测试工作有:

5.6.1 软件的每个开发阶段都要经过多种测试、试验的考核

故检系统软件必须通过静态分析、单元测试、系统综合试验、第三方评测、与飞船系统接口匹配试验、全箭匹配试验、全箭出厂试验等。

5.6.2 对软件的测试覆盖性提出定量要求

· 单元测试实现语句和分支 100%覆盖;

· 系统综合试验实现系统内接口测试的全覆盖;

· 与飞船系统接口匹配试验、全箭匹配试验、全箭出厂试验实现与外系统接口测试的全覆盖;

· 出厂前的测试项目覆盖靶场的测试项目。

5.6.3 为保证软件测试工作顺利开展,进行大量的准备工作

· 在软件测试前开展软件代码走查，检查软件代码和设计规格的一致性,检查代码规范性、可读性及逻辑的正确性;

· 对第三方评测的测试计划、测试细则、测试用例、测试结论进行评审。

6 结束语

经飞行试验证明，载人运载火箭故检系统软件全面采集了载人运载火箭的重要参数，准确反映了运载火箭的工作状态,能作出快速、有效的反应,其工作模式能够适应载人航天工程的需要，切实保障了航天员在上升段的生命安全。我们将继承一期工程故检系统软件工程的实践经验，在载人航天下一步任务中发挥更好的作用。 ◇