

doi: 10.7690/bgzdh.2016.09.013

软件逆向工程技术在 2.4 m 风洞核心控制程序研制中的应用

饶正周, 易凡, 金志伟, 杨兴锐

(中国空气动力研究与发展中心高速所, 四川 绵阳 622661)

摘要: 为解决 2.4 m 风洞核心控制程序中存在几个没有源代码的 C 语言执行模块严重制约系统平台升级的问题, 采用软件逆向工程技术研制新的替代模块。介绍了模块重新研制的步骤方法、软件调试方案等, 给出程序改造后的实际控制曲线。试验数据结果表明: 风洞流场和模型姿态控制精度达到或优于原来系统的指标, 并已投入风洞试验实际应用, 证明软件研制是成功的。

关键词: 风洞控制; 软件逆向工程; 控制程序; 研制

中图分类号: TP311.51 **文献标志码:** A

Application of Software Reverse Engineering Techniques in the Development of Core-control-program of 2.4 m Wind Tunnel

Rao Zhengzhou, Yi Fan, Jin Zhiwei, Yang Xingrui

(High Speed Institute, China Aerodynamics Research & Development Center, Mianyang 622661, China)

Abstract: To solve the problem that several C language executable modules without source code exist in the core-control-system program of 2.4 m wind tunnel which may severely hinders the future upgrade of the system, software reverse engineering techniques were adopted to develop the new sub-stititional module. Methods and procedures, debugging scheme through which the new modules were developed are depicted in detail and the actual control curve of the new program is also presented. The testing result data show that the control accuracy of flow field and model attitude is equal or better than that of the old software, and the newly developed modules has been put into use in the wind tunnel testing, so the development of the software is successful.

Keywords: wind tunnel control; software reverse engineering; control program; development

0 引言

2.4 m 风洞是我国自行研制的亚洲最大暂冲式跨声速风洞, 于 1997 年建成, 1998 年完成调试后投入正式科研型号试验, 其控制系统结构为基于局域网的分布式集散控制系统。上位监控机负责人机交互、状态监控, 下位 GE90-70PLC 是控制系统的核心, PLC 程序采用梯形图加 C 语言模块的混合编程方式进行设计。因为某些关键模块, 如主排同步控制、流场控制和模型姿态同步控制等算法相对复杂, 采用 C 语言实现更为高效便捷。但由于历史原因, 2.4 m 风洞 PLC 核心控制程序存在几个没有源代码的 C 语言程序编译后的执行模块。这些没有源代码模块的存在, 严重制约了控制策略的深度改造和优化, 特别是将来面临系统无法升级的严重问题。通过调研咨询得知, 该系统的 GE90-70PLC 系统已经停产, 必然要进行系统升级。但升级到新的系统平台则要求重新编译源代码, 没有源代码将无法实现升级。为做好现有系统升级换代准备, 必须

重新研制没有源代码的所有 C 模块。新研制的程序必须覆盖原有程序的全部功能, 马赫数控制精度必须达到或优于原来程序的精度水平。

软件逆向工程 (software reverse engineering) 又称软件反向工程, 是指从可运行的程序系统出发, 运用反汇编、系统分析、程序理解等多种计算机技术, 对软件的结构、流程、算法、代码等进行逆向拆解和分析, 推导出软件产品的源代码、设计原理、结构、算法、处理过程、运行方法及相关文档等。通常, 人们把对软件进行反向分析的整个过程统称为软件逆向工程, 把在这个过程中所采用的技术都统称为软件逆向工程技术; 因此, 笔者采用软件逆向工程技术研制新的替代模块。

1 2.4 m 风洞核心控制系统简介

2.4 m 风洞核心控制系统主要负责现场执行机构的静态单动、压力、流场和模型姿态等控制 (见图 1^[1])。程序主体架构采用梯形图编程, 但部分相对复杂算法采用 C 语言编程, C 语言经编译后得到

收稿日期: 2016-05-28; 修回日期: 2016-07-07

作者简介: 饶正周 (1967—), 男, 四川人, 高级工程师, 从事跨声速风洞测控技术与应用研究。

可执行的 EXE 模块，供 PLC 系统调用。程序中存在的没有源代码的主要模块共 5 个，见表 1。

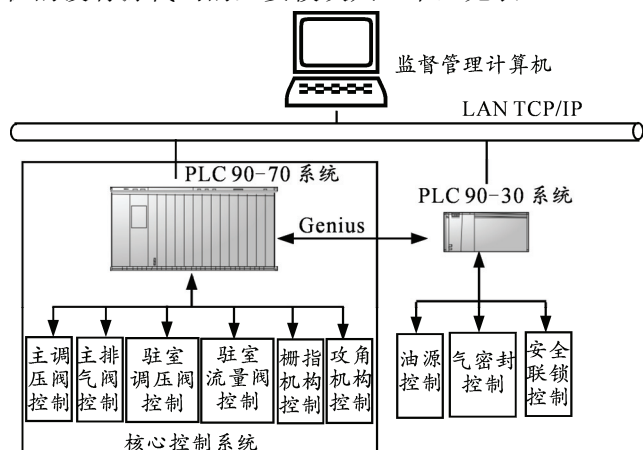


图 1 核心控制系统框图

表 1 无源代码模块

序号	模块名称	功能作用
1	LSUBM	连续变马赫数控制
2	ATKIC	全模攻角补偿控制
3	FUZZP	主排同步控制
4	SFF_IC	驻室抽气控制
5	ZTP_IC	主引和总压控制

2 核心控制程序逆向研制

2.1 逆向研制思路方法

2.4 m 风洞控制系统核心控制程序自 1997 年建成以来已使用近 20 年时间，其主要控制算法和参数是当年风洞调试时花费大量调试吹风车次的昂贵代价整定得到的，但这些参数有很多都在 C 模块里。采取何种研制方法能最大限度减少调试成本是必须考虑的问题。

一般来说，有 2 种方式可进行新的程序研制。一是完全推倒重来，另起炉灶，根据功能需求重新设计整个程序架构，并设计新的模块代替原来的没有源代码的 C 语言执行模块。该方法理论上可行，但由于程序代码复杂，功能繁多，加上核心控制程序直接与风洞现场执行机构、风洞流场等密切相关，调试工作量、占用风洞时间和吹风车次等成本将是高昂的，经论证认为工程上是不可行的。二是保持整个程序架构不做大的改变，采用以软件逆向工程为主的技术手段和方法，重新研制几个模块替代原来无源代码的 C 语言执行模块。如果配合恰当的调试方案，该方法将大大节省软件调试成本。

虽然这些模块没有源代码，但经过长期使用摸索，对程序的原理、功能和输入输出参数等有了比较充分的了解，加上结合以前的一些技术资料，对程序采用软件逆向工程技术手段进行研制是可行

的。现实中，人们并不总是完全需要逆向出目标软件的所有功能，因为将会是一个艰苦而漫长的过程。大多数情况下是意图通过对软件进行逆向，从中获取软件的算法，或破解软件及进行功能扩展等^[2-3]。限于篇幅，笔者主要以主排气阀(下面简称主排)同步控制模块 FUZZP 的逆向研制为例，阐述软件研制的思路方法，其余程序模块的研制方法大致相同。

2.2 主排同步控制模块逆向研制

所谓程序逆向研制，就是结合系统原理功能分析、程序理解和反汇编等多种技术手段，了解原来程序模块的功能原理、输出参数和具体变量操作等，设计开发出新的替代模块。

2.2.1 主排同步控制原理分析

要设计新的同步控制算法，首先要明确原来程序的功能原理(参见图 2)。主排气阀系统由 1[#]、2[#]、3[#]、4[#] 4 个排气阀门组成，4 个阀门必须同步运行，同步误差小于 1 mm，共同完成吹风试验中对总压的控制。

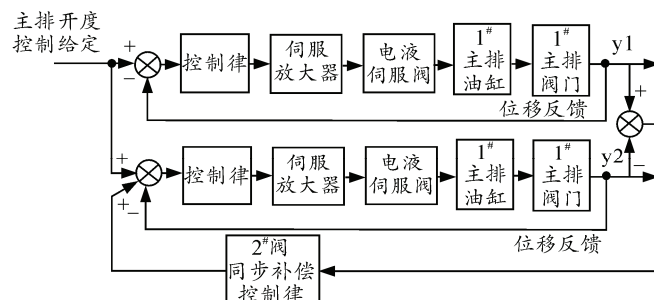


图 2 主排气阀同步控制原理

主排开度控制环作为总压闭环的内环。通过对原有程序分析，FUZZP 模块主要实现 4 个主排开度同步控制功能。从图 2 可见，控制策略为其他 3 个主排跟随 1[#] 主排的主从控制模式。以 2[#] 主排为例，其跟随 1[#] 主排的控制原理框图如图 3 所示。其他 3[#]、4[#] 号主排跟随原理与 2[#] 主排相同^[4]。

了解了主排同步控制基本原理后，即可着手采用梯形图语言和 C 语言设计主排同步控制的基本架构和具体控制功能。

2.2.2 反汇编跟踪分析

程序主体架构及功能完成后，要解决的主要问题是保证程序输入输出参数与原来的程序模块保持一致。更重要的是，当初开发设计程序的时候并未严格遵守模块化编程的规范，采用了在模块内

部直接对模块外部 PLC 地址变量进行读写操作的方式，这些变量不搞清楚，新的程序就无法完全替代原有模块。因为没有源代码，就只能采用反汇编跟

踪的方式进行分析，确定程序中是否直接对模块外部 PLC 变量进行了读写操作，以及对哪些变量进行了读写操作。

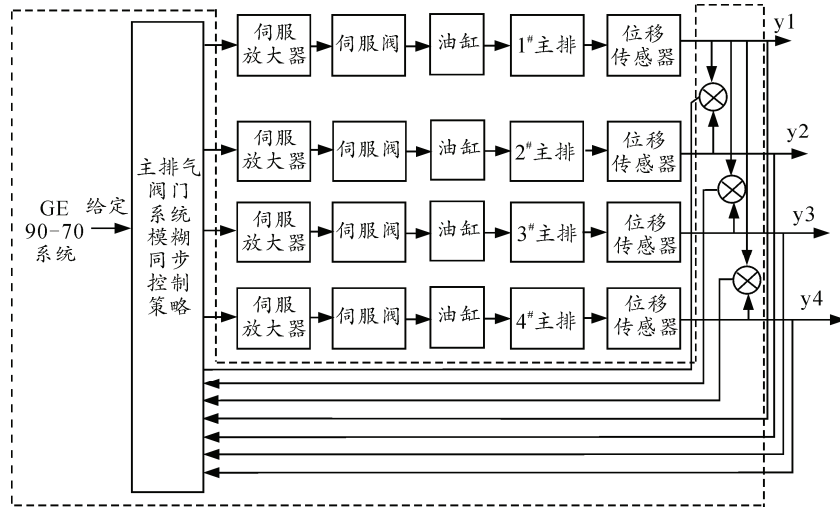


图 3 2#主排跟随 1#主排控制框图

采用 W32Dasm 反汇编工具软件对原 FUZZP 模块的执行代码首先进行静态反汇编，初步了解 PLC 调用的 EXE 执行文件的结构^[5]。笔者首先采用如下最简 C 语言程序结构的调试程序 Test.c:

```
#include "plcc9070.h"
main (void)
{
    BIT_SET_M(7029); //7029M 置位
    BIT_TST_M(7028); //7028M 位测试
}
```

对其编译生成 PLC 可识别的执行文件 Test.exe。然后对该执行文件进行反汇编，这样便于弄清该程序的执行文件结构，从而确定 PLC 调用 Test.exe 文件的参数传递、地址跳转、变量分配、函数执行和结果返回等基本结构和流程^[6-7]。了解这些基本要素后，就可如法炮制对主排控制模块 FUZZP 进行反汇编分析，再结合程序在 PLC 实际运行中进行跟踪。确定主排同步控制模块中直接对模块外部 PLC 变量进行操作的有以下 2 个：1) 5103 M 点置位；2) 5104 M 点置位。

这 2 个 PLC M 点的置位非常重要，是程序中其他语句运行的触发条件。弄清了这些情况后，在新的程序里作相应处理，就成功解决了新旧程序的参数对接问题。

2.2.3 程序静动态调试

对 2.4 m 这样的大型暂冲式风洞来说，一次吹风调试的成本很高，采取何种方案进行调试就显得

格外重要，甚至关系到整个研制方案是否可行。

根据该风洞控制系统的实际情况，笔者制定了如图 4 所示的调试思路和方案。全部模块研制完成后，结合日常风洞试验任务，新老模块同时运行，但新研制的模块不投入实际控制。通过试验数据、控制曲线和变量监控等手段分析对比新研制模块的输入输出参数以及对 PLC 变量的操作等是否与原来的程序模块保持一致，如不一致，则分析查找问题，修改程序后继续调试，直到新老模块输入输出参数保持一致，新的模块才能投入实际应用。检验新模块是否满足要求的最终标准：洞流场马赫数精度、模型姿态角精度达到或优于原来程序的水平。

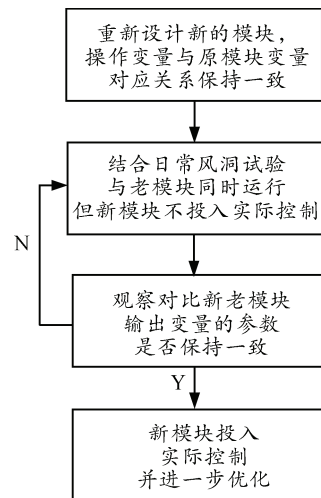


图 4 程序调试思路方法