文章编号:1671-4598(2014)11-3494-03　　中图分类号:TP274　　文献标识码:A

温箱控制器的运行控制文件测试与研究

杨光年

(中船重工 716 研究所 连云港杰瑞深软科技有限公司,江苏 连云港　222006)

摘要:为了建立综合控制台对温度试验箱进行集中控制,需要对各独立的温控试验箱的运行文件进行分析和整合,形成可被温控试验箱执行的 *.PRG 程序文件。方法是首先通过原系统操作界面程序,设定温箱工作温度和时间,产生一个温箱控制器执行的 *.PRG 文件。然后,用 Beyond Compare 工具,对此(二进制)文件进行测试分析,得出文件的开始标志,温度阶梯步数,温度值单元,温度点切换时间单元,切换点行标志和文件结束标志等 6 个部分的位置关系,从而获得温箱控制器运行文件 *.PRG 的内部结构。根据文件内部数据结构关系,可以建立符合原 *.PRG 文件格式且可通用的可执行程序文件。在某型综合控制台的设计中采用该方法建立的 *.PRG 文件对各试验箱进行独立运行实验,实现了对温箱的综合控制。

关键词:数据格式;程序;二进制文件

Test and Research of Operation Control File for Temperature Controller

Yang Guangnian

(Lianyungang Jari DeepSoft technology Co., Ltd., CSIC 716 Research Institute, Lianyungang　222006, China)

Abstract: In order to establish an integrated console for centralized control of temperature test chamber, it needs to analyse and integrate for the running file of separate temperature-controlled test chamber so that can be performed a *. PRG program file. First, it sets work temperature value and time of temperature chamber through the operation interface of original system to format a executable *. PRG file for the thermostat controller. And then, using Beyond Compare tool to test and analyse the (binary) file in order that it can draw location relationship of six parts including the file start flag, the temperature stepped number, the temperature value position unit, the temperature point switching time, the temperature switching point line flags, and the file ending sign and so on. So it can derive the internal structure of running *. PRG file from thermostat controller. According to the documents of internal data structures, a general executable file which meets the original format requirements is established. In the design of a certain type of integrated console, the *. PRG file through the above method formatted is used to the test of each independent temperature chamber that achieves a comprehensive control for each temperature chamber.

Keywords: data format; program; binary file

0　引言

在我国航天、国防军工等单位,大量使用着国外进口的温度试验箱,这些试验箱都是由计算机独立控制,可以完成产品设定的各种高低温和湿度等特定试验,达到检测和鉴定效果[1]。如果试验箱比较多,频繁的进行各种试验,试验箱的参数设定、记录就需要大量人员工作。

假如建立一个综合温度控制系统,及时对各独立的温度试验箱数据进行监控、保存和处理,这将极大方便和减轻工作人员的劳动强度。目前,在我国,对国外试验箱进行集中控制管理还未进行相关研究,因此,开展这方面的研究意义深远。

建立综合控制系统的关键步骤是如何获取试验箱的内部运行文件,即试验箱的运行控制程序,但产品并未提供确定试验箱控制程序的相关接口资料。通过试验操作,发现每次设定温度控制程序时,均需要给程序文件设置一个名称,比如“TT”,后缀名是 *.PRG。而产生的 TT.PRG 文件就是试验箱温度控制文件,试验箱的控制完全按这个文件进行。

在综合控制台建立 PRG 程序文件,取代试验箱上的操作,是实现综合控制的核心。由于各试验箱都是由国外进口的,PRG 文件是系统内部不对外开放的二进制可执行文件[2]。所以,确定 PRG 文件格式和相关参数,只能根据试验箱的操作流程进行,从而判别试验箱在进行温度试验时是根据该程序文件进行温度控制的。因此,如果对多个试验箱进行综合控制,就必须对 PRG 文件进行测试分析。

Beyond Compare 3[3] 工具软件 ,可以支持普通文本、代码、十六进制文件等进行比较分析。对于开发者,可以用它来对比两份代码的变化,确定参数值的位置。由于 *.PRG 文件是一个二进制的可执行文件,可采用 Beyond Compare 3 工具对 PRG 文件进行打开,选择十六进制比较方式,分析测试 *.PRG 文本。

1　从独立试验箱产生一个 *.PRG 文件,查看 PRG 文件格式

为了分析测试 .PRG 文件,先设定几个温度点值,通过温箱控制器生成温度控制程序。比如给定温度点值 30 ℃,50 ℃和 0 ℃,各温度点的保温时间都设置为 2,3 和 1 分钟。温箱温度从室温开始上升到 30 ℃,温度保温 2 分钟,然后,又使温度上升到 50 ℃,保持 3 分钟时间,最后降温到 0 ℃,保持 1 分钟。通过这样一个温箱升温的简单温度控制过程,查看温度控制文件的格式及温度变化内容,对形成的独立的 *.PRG 文件,取名为 TT.PRG。再建一个 TT1.PRG 文件,温度变化的值是 50 ℃,30 ℃,10 ℃,仍采用上述确定的工作时间。然后,用 Beyond Compare 3 工具软件进行打开,如图 1 所示。

收稿日期:2014-04-16;　**修回日期**:2014-05-14。

作者简介:杨光年(1965-),男,江苏连云港人,高级工程师,主要从事智能控制软件和物联网方向的研究。

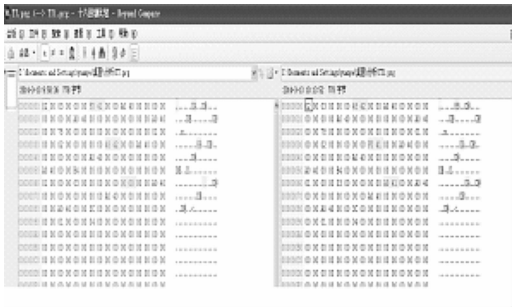

图 1　简单的 PRG 文件

1.1　文件头分析

查看两个文件 TT. PRG 和 TT1. PRG 文件的相同处和不同处。发现两个文件的第一个字节都有十六进制数 02H 数据，把它与 ASCⅡ码表对比，表示正文开始。标明温控文件 PRG 的头文件，再生成几个 *. PRG 文件，实验发现都在第一个字节存在十六进制数 02H。因此，可以断定 02H 是 *. PRG 文件的规定格式，并且位置在第一个字节上。

温度控制步骤分析：

文件 02 单元内容是 03H，这个值通过多个生成的 PRG 文件对比，发现代表的是温度设置的步骤总数，这里 03H 代表温度设定了 3 步，比如开始给定的温度值 30 ℃，50 ℃和0 ℃，第一步 30 ℃，第二步 50 ℃，第三步 0 ℃结束，共 3 步。因此这个单元存放温度设置的总步数。

1.2　温度值位置分析

TT. PRG 文件中的 06 和 07 单元是温度值的整数单元，在这两个单元中存放着温度值的整数，比如 30 ℃，在 06 和 07 单元中内容是 F0H 和 41H，04 和 05 单元存放着温度值的小数部分。

TT1. PRG 文件是与 TT. PRG 文件对应的文件，温度点变化是 50 ℃，30 ℃，10 ℃。温度的变化正好与 TT. PRG 相反（TT. PRG：30 ℃，50 ℃，0 ℃），目的是分析出同样的温度值因顺序不同会有什么变化位置。通过实验可知，50 ℃的代表值是 42H 和 48H，30 ℃的代表值是 F0H 和 41H，而且在表中存放顺序是低位在前，高位在后。温度点的位置分别以 06H 和 38H 两个单元为起点，两个温度点的位置差是 38H－06H＝32H，即 50 位。查看第 3 个温度值在表中的位置是 6AH，第 3 个温度点与第 2 个温度点的位置差计算结果是 6AH－38H＝32H，也是 50 位。为了证明温度点的位置差是 50，测试其它几个 *. PRG 文件，实验结果一致。

1.3　温度值整数和小数位置分析

温度值的整数部分存放在高位，小数部分存放在低位。起始点以整数位置为准，整数位置的低 2 个字节是小数部分的存储单元。小数部分的值是相邻两个温度值之间的数据，一般热电偶测温数据表给出的是每一度的温度对应表，小于 1 度的值是通过计算获取的，计算获得值转换为十六进制小数，依此存放到指定单元中。

1.4　温度点切换行标志分析

在 TT. PRG 和 TT1. PRG 文件中，可以看到有 01 00 00 00 02，01 00 00 00 03，01 00 00 00 04 等字符串，它们分别表示温度点的切换行。01 00 00 00 02 表示第 2 步，01 00 00 00 03 表示第 3 步，01 00 00 00 04 表示第 4 步，01 是标志位，02，03，04，…分别代表第几步。在 TT. PRG 文件中，第 1 步 30 ℃，第 2 步 50 ℃，第 3 步 0 ℃。也可以依此字符串来确定温度值小数部分的存储位置，即在表示步数的字符位置后，第 4 个字节起存放小数部分，共两个字节。

标志温度点切换行的字符串位置分别是：2EH，60H，92H。以这 3 个字符串的起始位置计算它们的位置差：60H－2EH＝32H，92H－60H＝32H，得到字符串起始位置差是 50 位。即每隔 50 位便是新的一行切换点。因此，在设计 PRG 文件时，可以将 01 00 00 00 02 放置在起点在 2EH 单元，之后 50 位的位置存放 01 00 00 00 03，依次类推，有几步，就设置几行切换点。

1.5　温度点的控制时间和单元分析

在 TT. PRG 和 TT1. PRG 文件中，存放第一个温度点的时间单元是 22H，内容是 78H，存放第二个时间点单元是 54H，内容是 B4H，存放第三个时间点的单元是 86H，内容是 3CH。时间点单元的位置差计算：54H－22H＝32H，86H－54H＝32H，换算为十进制的值等于 50。因此，可以确定在 22 单元，存放第一个时间值，然后每隔 50 位是下一个时间点单元，直至最后一个时间点位置。在进行温度值设定时，在操作界面上设定时间分别是 2 min，3 min 和 1 min。在 22H，54H，86H 单元中的内容分别是 78H，B4H，3CH，换算为十进制数分别是 120 s，180 s，60 s，化为分钟数正好是 2 min，3 min，1 min，完全吻合。

1.6　文件结束标志分析

在 TT. PRG 和 TT1. PRG 文件中，都有最后一段字符串：2A 2D 2D 2A 0B AD F0 0D 02 00 04 00 0A 00，它是 PRG 文件的固定格式，标志 PRG 文件的结束，见图 2，但字符串中的第 11 个字节存放的内容是 04H，是温度控制执行步骤总数：4。在设计 PRG 文件时一定要把温度控制总步数写入这个字节单元中，然后再把处理好的固定格式写人创建的 PRG 文件中。

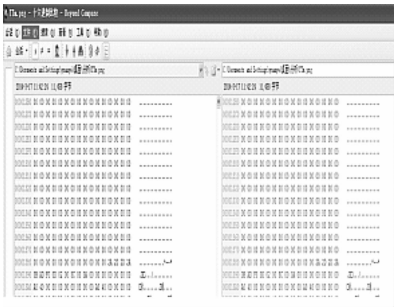

图 2　PRG 文件的结尾

通过对 PRG 文件的测试分析，基本获得了 PRG 文件的内部格式，即由正文标志开始，温度阶梯步数，温度点值，温度点切换行标志，温度切换时间和正文结束标志等共 6 个部分组成。其中，温度点值、温度点切换行标志和温度切换时间是文件的核心，会根据温度点的设置，在 PRG 文件中重复出现多次，次数由温度点值的阶梯步骤总数确定。

掌握上述几个关键点及存放数据的格式，就可以利用编程工具，创建和生成一个 PRG 文件，供独立温箱控制器使用，实现温箱的综合控制，从而实现对产品的二次开发和创新。

2　其它温度值的获取

创建 PRG 文件，需要设置温度点的值。而每一个温度点

都有可能会被用到，这就要求知道每一个温度点的转换值。要确定这些温度点值，可通过独立试验箱控制器操作界面，设置连续的温度点，形成一个 PRG 文件。在这个 PRG 文件中，根据温度点位置，查出每一个温度转换值的数据，逐个把它们从 PRG 文件中取出，从而建立查表文件，以此在综合控制创建 PRG 文件时进行查表使用。

实验方法是，先设定连续的温度值，范围在：1 ℃，2 ℃，3 ℃，…，100 ℃，建立起 1 ℃到 100 ℃的温度值 PRG 文件，见图 3。查看 1 ℃到 100 ℃温度转换值在 PRG 文件中的对应位置的参数数据，负数也是照此处理，就可得到 －100～100 ℃连续温度点值的数据。

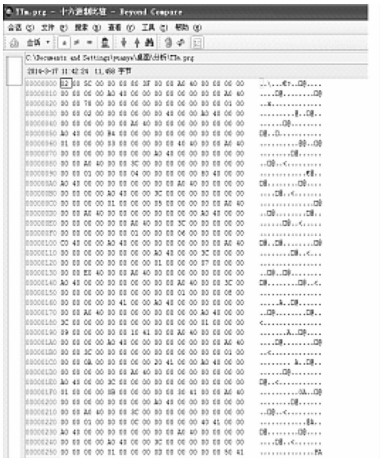

图 3　1 ℃到 100 ℃的 PRG 文件

通过这样一个表，可以得出 1 ℃，2 ℃，3 ℃，…，100 ℃在 PRG 文件中的十六进制数，根据先前确定数据位置，从第一个温度值位置 06 单元起，依次间隔 50 位，连续取 100 次，每个温度值取 2 个字节，即可建立温度值转换参数表，见表 1。

表 1　1°到 100°连续温度值对应参数表

温度值	十六进制	温度值	十六进制	温度值	十六进制	温度值	十六进制	温度值	十六进制
1	3F80H	21	41A8H	41	4224H	61	4274H	81	42A2H
2	4000H	22	41B0H	42	4228H	62	4278H	82	42A4H
3	4040H	23	41B8H	43	422CH	63	427CH	83	42A6H
4	4080H	24	41C0H	44	4230H	64	4280H	84	42A8H
5	40A0H	25	41C8H	45	4234H	65	4282H	85	42AAH
6	40C0H	26	41D0H	46	4238H	66	4284H	86	42ACH
7	40E0H	27	41D8H	47	423CH	67	4286H	87	42AEH
8	4100HD	28	41E0H	48	4240H	68	4288H	88	42B0H
9	4110H	29	41E8H	49	4244H	69	4278AH	89	42B2H
10	4120H	30	41F0H	50	4248H	70	428CH	90	42B4H
11	4130H	31	41F8H	51	424CH	71	428EH	91	42B6H
12	4140H	32	4200H	52	4250H	72	4290H	92	42B8H
13	4150H	33	4204H	53	4254H	73	7292H	93	42BAH
14	4160H	34	4208H	54	4258H	74	4294H	94	42BCH
15	4170H	35	420CH	55	425CH	75	4296H	95	42BEH
16	4180H	36	4210H	56	4260H	76	4298H	96	42C0H
17	4188H	37	4214H	57	4264H	77	429AH	97	42C2H
18	4190H	38	4218H	58	4268H	78	429CH	98	42C4H
19	4198H	39	421CH	59	426CH	79	429EH	99	42C6H
20	41A0H	40	4220H	60	4270H	80	42A0H	100	42C8H

这就不需要知道特定算法，直接设置温度点，以文件操作方式，自动生成连续的温度点转换值参数的方法。通过这样的方法，就摆脱了只有依据特定算法和电路计算，才能获取 PRG 文件温度点值的要求。

负数温度值范围：－100 ℃，－99 ℃，－98 ℃，－97 ℃，…，－3 ℃，－2 ℃，－1 ℃也可按此方法建立表格。

根据表 1，就可以设计温度值在 PRG 中的表示格式。两度之间的小数部分可以十进制小数表示存放到整数单元的前两个单元中，比如 10.3 ℃，采用十六进制表示，整数查表为 4120H，小数 0.3 转换为十六进制小数，表示为 .4CCCH。在 PRG 文件中存放顺序是前两个字节放小数部分，后两个字节放整数部分，低字节在前，高字节在后，比如：10.3 ℃在文件中形式为 CC C4 20 42。

需要说明的是搞仿制，尤其是国外产品，不可能获得产品制造商的技术资料。本文研究的是温箱控制器的运行控制程序，温度转换值的计算是跟温度传感器采用的热电偶有关[4-5]，热电偶的温度转换是商家根据外围线路确定的，因此不可能收集到这方面的资料。

所以借助其产品，生成一系列温度值数据，是仿制产品的捷径。

3　编程文件设计

按照 PRG 文件的格式，及数据单元位置和内容，可以利用编程软件实现具有 PRG 文件格式的运行控制文件。程序流程图如下：

1）建立文件，设置为二进制方式；
2）写入正文开始标志位 02H；
3）接着在 02 单元写入温度设定的总步数；
4）在 06，07 单元写入第一个温度点值；
5）接着写入换行标志位；
6）写入温度点值；
7）每隔 50 位，写入温度点值到这个单元中。

重复这几个步骤，当温度点设置完成后，在 PRG 文件中插入文件结束字符串，完成全部 PRG 文件的创建。

4　结论

温度控制运行文件，尽管它是二进制文件，但也是可以认识和有规律可循的。通过对运行控制文件的分析，就可以在综合控制台上设置温箱控制的运行程序，达到综合控制和运行各温箱的目的。本文对温度控制文件的认识分析过程还处于一般认识阶段，更深更广的见解，还需科研人员的大量参与，随着问题的深入研究，更多更好的方法会涌现出来，这对推动产品的开发和创新，更快学习国外的新技术有着十分重要的意义。

参考文献：

[1] 于　洋. 高低温试验箱微机自动系统的设计 [J]. 工业仪表与自动化装置，2003，(2)：54－56.
[2] 李广旭，李伟华，潘　炜，等. 软件安全逆向分析中程序结构解析模型设计 [J]. 计算机工程与应用，2008，44 (32)：64－67.
[3] Greg Steen. Compare，Merge And Synchronize Files And Folders：Beyond Compare 3 [J]. TechNet Magazine，2009，5 (11)：193－195.
[4] 马江涛. 单片机温度控制系统的设计及实现 [J]. 计算机测量与控制，2004，12 (12)：1219－1221.
[5] 张苏英，庞志锋，魏领琴. 集成温度传感器在热电偶温度补偿中的应用 [J]. 仪器仪表学报，2003，23 (3)：112－112.