

计
算
机
应
用

轨道交通信号系统安全计算机浅谈

唐俊同

(株洲南车时代电气股份有限公司 安全装备事业部, 湖南 株洲 412007)



作者简介：唐俊同（1977-），男，工程师，从事轨道交通信号系统安全装备研究。

摘 要：描述了轨道交通信号系统安全计算机的发展历程、技术难点以及安全计算机在我国的应用情况，并对二乘二取二结构安全计算机、三取二结构安全计算机、编码处理器安全计算机的有关特点进行了比较。

关键词：安全计算机；ATP；轨道交通；信号系统；编码算法

中图分类号：U264.4⁺2；TP391 **文献标识码：**A **文章编号：**1000-128X(2011)06-0073-03

Brief Presentation on Vital Computer for Rail Transit Signal System

TANG Jun-tong

(Safety Equipment Business Unit, Zhuzhou CSR Times Electric Co., Ltd., Zhuzhou, Hunan 412007, China)

Abstract: Development course, technical difficulties and domestic applications of vital computer for rail transit signal system were described. Characteristics of double 2 vote 2, 2 out of 3, encode processor vital computer were compared.

Key words: vital computer; ATP; rail transit; signal system; encode algorithm

0 引言

安全计算机是轨道交通信号系统相关安全装备的重要组成部分，为列车的安全运行提供强有力保障。

在轨道交通信号系统领域，大致存在3种不同结构的安全计算机：基于二乘二取二结构的安全计算机、基于三取二结构的安全计算机以及基于安全编码单处理器结构的安全计算机。

1 发展历程

早期的控制设备不采用多重冗余，也不具备故障-安全的概念，仅为实现某一特定领域而产生的特定应用，其原理结构如图1。



图1 早期系统模型

由于设备运行在比较恶劣环境中，比如强电磁干扰、恶劣的散热条件、低温环境、长期振动等，甚至是很多恶劣条件的组合，系统容易产生故障并导致系统失效，这种单一系统的可靠性面临着严峻的挑

战。

为了更好地解决可靠性的问题，人们进行了新的探索，采用2套CPU进行冗余，设计出基于二机备份结构的设备，单一故障后不导致系统失效，提高了系统可靠性，如图2所示。

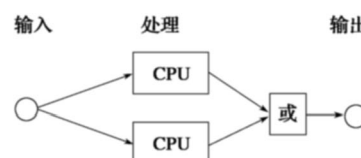


图2 二机备份可靠冗余结构

二机备份结构解决了可靠性问题，但无法解决2个CPU计算结果不一致的问题。为解决该问题，提出了二取二结构，对2个CPU的运算结果进行比较，比较结果一致后输出，不一致则导入到故障状态，提高了系统的安全性。二取二的结构如图3所示。

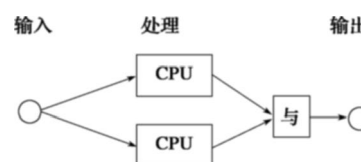


图3 二取二安全冗余结构

基于备份结构，将其CPU用二取二结构进行替换，演绎出目前在世界范围内广泛使用的二乘二取二的安全可靠计算机系统结构，如图4所示。

收稿日期：2011-04-29；收修改稿日期：2011-08-01

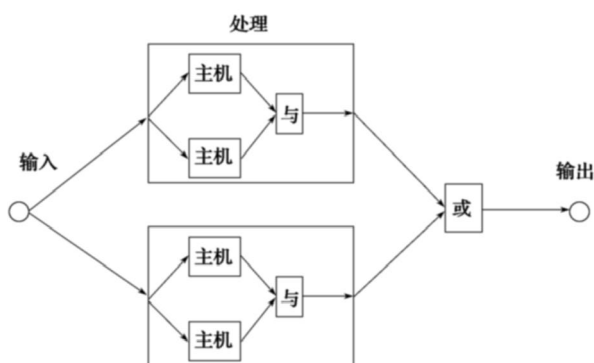


图4 二乘二取二安全冗余结构

与二乘二结构的安全性及可靠性处于相同数量级并且广泛使用的另外一个冗余结构是三取二安全可靠冗余结构,如图5所示。

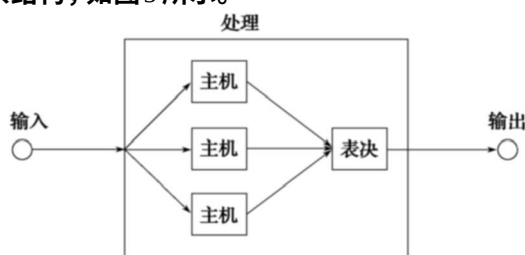


图5 三取二安全可靠冗余结构

不论是三取二结构还是二乘二取二结构,均以增加系统复杂性为前提。

为了简化系统设计,同时又不失安全性,在1987年3月,法国运输部门召集了不同领域(铁路、地铁、核能、航空、政府部门、大学院校等)的专家组成国家安全委员会,开展单编码处理器的安全评估,于1989年给出了编码处理器模块安全鉴定。随后该技术很快被用于巴黎RER地铁快速线A线以及Laon的POMA系统的ATP设备,以及芝加哥VAL的轨旁设备。

编码处理器的安全操作基于信息冗余概念,采用故障检测码识别各种类型的微处理器失效以及编译器错误。故障检测码的基本单元为32位的信息码D外加48位的检测码(C1,C2)。编码处理器对所执行的每条程序代码进行检查,采用单个CPU通过软件用数学的方法保证系统安全。为了保证系统可靠性,通常采用2套设备进行冗余。

2 安全计算机的技术难点

2.1 二乘二取二结构安全计算机

二取二的数学模型为

$$OUT_x = F_CPU_x (IN_x) \quad (1)$$

$$OUT_y = F_CPU_y (IN_y) \quad (2)$$

$$OUT_{safe} = (OUT_x \cap OUT_y) \quad (3)$$

式中: IN_x 表示CPU_x处理的输入信息; IN_y 表示CPU_y处理的输入信息; F_CPU_x 表示CPU_x的处理过程; F_CPU_y 表示CPU_y的处理过程; OUT_x 表示CPU_x处理的结果; OUT_y 表示CPU_y处理的结果; OUT_{safe} 为2个CPU计算

结果进行表决后本系统最终输出。

二乘二取二采用2套二取二进行系统级冗余,每套二取二称为一系。

①系内各CPU输入数据的一致性

根据式(3)可知,要想 OUT_{safe} 安全侧有输出,则要求 OUT_x 与 OUT_y 一致。假设 F_CPU_x 与 F_CPU_y 均能正常地执行正常的功能,则要求 IN_x 与 IN_y 一致。

有些系统在2个CPU每次计算之前进行一次数据交换,其主要目的就是为了保证系内各CPU输入数据的一致性。

②系内双机同步

系内双机同步的最终目的也是为了避免系内各CPU输入数据的不一致。假如系内双机不同步,一个CPU执行的是上周期的输入数据,而另外一个CPU执行本周期的输入数据。该情况下,即使CPU能正常执行功能,也可能直接导致比较结果异常。

日本系统的二取二结构采用一个晶振驱动2个CPU,通过硬件实现了双机的指令级同步,不过这对比较与表决提出了更高的要求。

③二取二表决的安全性

根据式(3)可知,即使 OUT_x 与 OUT_y 一致,如果 $\cap$ 操作有问题,也将导致系统失效,这也是二取二需要解决的核心关键技术。有些系统采用硬件表决,有些系统采用软硬件结合完成表决功能。

2.2 三取二结构安全计算机

三取二的数学模型为

$$OUT_x = F_CPU_x (IN_x) \quad (4)$$

$$OUT_y = F_CPU_y (IN_y) \quad (5)$$

$$OUT_z = F_CPU_z (IN_z) \quad (6)$$

$$OUT_{safe} = (OUT_x \cap OUT_y) \cup (OUT_x \cap OUT_z) \cup (OUT_y \cap OUT_z) \quad (7)$$

式中: IN_z 表示CPU_z处理的输入信息; F_CPU_z 表示CPU_z的处理过程; OUT_z 表示CPU_z处理的结果; OUT_{safe} 为对3个CPU计算结果进行表决后的最终输出。

三取二安全计算机的关键技术点有:

①输入数据的一致性

由式(7)可知,要想获得安全的输出,至少要求3项输出中的2项一致;在 F_CPU_x 、 F_CPU_y 、 F_CPU_z 均能行使正常功能的前提下,至少要求3个输入中的2个完全一致。

大部分三取二系统在CPU每次计算之前进行一次数据交换,其主要目的也是为了保证各CPU输入数据的一致性。

②三机同步

三机同步的目的与二乘二取二结构中的双机同步相同,也是为了确保输入数据的一致性。

不过在三取二系统中,允许存在1个CPU与另外2

个不一致。在这种情况下，三取二将降级为二取二，但不影响系统的安全性。

③三取二表决的安全性

三取二表决的安全性同二取二一样，一旦表决器出问题，则前期工作付诸东流。三取二的安全瓶颈关键在表决器的安全性。

2.3 编码处理器安全计算机

1) 编码算法

与三取二和二取二不同，基于编码处理器的单CPU安全计算机的关键技术点不在同步，也不在表决，而在于编码算法以及如何运用该算法确保程序数据流及控制流的安全检查。

编码算法的基本原理：

软件中任何变量 X 由2个域(X_f, X_c)组成，其中 X_f 为32位功能码， X_c 为48位检测码。功能码与检测码结合形成安全码。

软件中的数据都将被转换成安全码，任何针对数据的算术运算和逻辑运算都需要研究一套机制转换为对安全码的运算，所有控制流也需要开发对应安全软件模块，最终的应用都可以基于这些基本模块进行二次开发。

编码算法能检测的故障有以下4种类型：

①检测运算错误。

采用一个整型常量 A ，使得安全数据 $X(X_f, X_c)$ 满足以下等式：

$$2^k X_f + X_c = 0 \pmod{A}, A \approx 10^{14}$$

式中： X_f 为原始数据； X_c 为校验码，对 X_f 以 A 值取模后得到 X_c 。

②在上述算式基础上增加一个签名 B_x ，用于检测运算数错误或地址错误。

$$2^k X_f + X_c = B_x \pmod{A}$$

③再增加一个时间用于检测时序错误。

$$2^k X_f + X_c = B_x + D \pmod{A}$$

④最后增加一个TRACER变量，用于检测控制流错误。

2) 数字量输入信息编码

为了不降低安全计算机的安全性，实现系统安全，需要采用特定的编码电路，对数字量输入数据 X_f 采用 $X(X_f, X_c)$ 的形式按照安全计算机的要求进行编码。同时为了区分每个时序的不同输入，还可增加时间参数Date用于检测时序错误。

3) 数字量输出信息解码

与数字量输入信息编码阶段相反，需采用特定的

解码电路，对安全计算机计算的数字量输出 $X(X_f, X_c)$ 的信息进行解码，还原成外设所能识别的 X_f 的形式。同时为了区分每个时序的不同输出，增加时间参数Date用于检测时序错误。

4) 安全侧处理

安全编码计算机故障或检测出故障后，必须采用故障安全原则，将系统导向安全侧。

3 不同安全计算机的比较

不同安全计算机的比较见表1。

表1 不同结构安全计算机比较

项目	二乘二取二	三取二	编码处理器
安全性	高	高	高
可靠性	高	高	通过冗余实现高可靠
硬件复杂度	高	高	低
软件复杂度	高	高	高
工艺要求	高	高	低
体积	大	大	小
设备造价	高	高	低
维护成本	高	高	低

4 安全计算机在我国信号系统中的应用

历次铁路大提速对我国的装备制造业产生了深远影响，安全计算机广泛地应用于轨道交通信号系统各设备。具体情况为：CTCS2-200H型ATP设备采用二乘二取二结构安全计算机；CTCS2-200C型ATP设备采用三取二结构安全计算机；CTCS3-300S型ATP设备采用二乘二取二结构安全计算机。计算机联锁系统采用二乘二取二结构安全计算机；LEU（轨旁电子单元）设备采用编码处理器安全计算机；临时限速服务器采用二乘二取二结构安全计算机。

5 结语

随着铁路的快速发展，科研人员对安全计算机技术的研究也越来越深入。希望在不远的将来，具有中国自主知识产权的安全计算机能够走向国门，跻身世界安全计算机行列。

参考文献：

- [1] 赵志熙. 计算机联锁系统技术[M]. 北京：中国铁道出版社，2008.
- [2] Ozello Patrick. THE CODED MICROPROGSSOR CERTIFICATION [DB/OL]. Safety of computer control systems 1992 (SAFECO MP'92)[2004-04-20].