doi: 10.7690/bgzdh.2016.10.001

遥码通信系统的反设计和国产化研究

姜广顺[1]，金芮芃[2]，曹佩武[1]，冯　云[1]，李　晓[1]，杨国平[1]
（1. 空军二十三厂研究所，北京 102200；2. 天津光电通信技术有限公司技术中心，天津 300211）

摘要：为实现遥码通信系统的国产化功能替换，提出一种基于逆向工程方法和嵌入式控制技术的新思路。通过对原遥码通信系统的组成、功能分析和反设计，运用逆向工程方法和嵌入式控制技术，实现了遥码通信系统的国产化。在专用测试台上，对国产化遥码通信系统与原遥码通信系统进行了性能对比测试。试验结果证明：国产化遥码通信系统能够满足武器装备的正常使用要求，已成功应用于工厂装备修理和部队装备的维护保障，减少了对装备引进方的依赖，有效缩短了装备维修周期，节约了维修成本。

关键词：遥码通信系统；反设计；国产化；逆向工程方法
中图分类号：TJ02　　**文献标志码**：A

Research on Localization and Inverse Design of Remote Communication System

Jiang Guangshun[1], Jin Ruipeng[2], Cao Peiwu[1], Feng Yun[1], Li Xiao[1], Yang Guoping[1]
(1. *Institute*, *No.* 23 *Factory of PLA Air Force*, *Beijing* 102200, *China*;
2. *Technology Center*, *TOEC Technology Co*., *Ltd*, *Tianjin* 300211, *China*)

Abstract: In order to realize the localization function replacement of remote communication system, a new idea is proposed based on reverse engineering method and embedded control technology. The localization of remote communication system is achieved through composing and function analyzing to the original one, using reverse engineering method and embedded control technology. On the special test bed, the performance compare test between the localized system and the original one is carried out. The tryout result indicates that the localized system can meet the application requirement of the imported weapon equipment, and it has been used in a factory and in the army to guarantee equipment maintenance and support. The reliance on the exporter is reduced, the maintenance cycle of the equipment is shortened effectively, and maintenance cost is saved, too.

Keywords: remote communication system; inverse design; localization; reverse engineering method

0　引言

某引进型号指挥自动化系统，采用搜索雷达、指挥控制和通信三位一体技术[1]，可对 6 个火力单元实施指挥控制。作为指挥自动化系统核心设备的遥码通信系统(以下简称“原遥码通信系统”)，随使用年限的增长，故障率增高，备件消耗量越来越大。由于后续备件的订货渠道不畅，开展备件国产化研制是解决引进装备维修保障的有效途径[2]。

原遥码通信系统设计思想独特，工作原理以及信号时序关系复杂，特别是电路中采用了许多专用芯片(器件)。显然，不能采用“一一替换”的研仿模式，必须对原遥码通信系统在不同工作状态下的输入、输出信息进行系统地测试、分析和处理，尽可能得到其完整、准确的控制时序和工作流程后，才能对其进行功能替代[3]；因此，笔者采用逆向工程方法并运用单片机、嵌入式控制技术，实现原遥码通信系统的国产化。

1　原遥码通信系统的组成及功能

遥码通信系统由指挥自动化系统作战指挥车设备舱中的主站和火力单元制导雷达指控舱中的从站 2 部分组成，作战指挥车同时与 6 个制导雷达进行遥码信息交换。指挥自动化系统通过发送目标指示、状态转换控制、天线调转等指令对火力单元实施指挥控制，进行目标分配；通过接收各制导雷达上传的火力单元工作状态、制导雷达天线方位、目标和弹药通道状态、通道目标诸元等信息，实时掌控火力单元的工作情况。原遥码通信系统构成，见图 1。

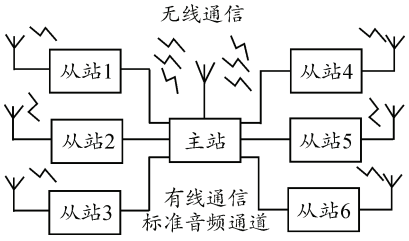

图 1　原遥码通信系统构成

2　原遥码通信系统的功能分析和反设计

2.1　编码方式

原遥码通信系统有 3 种通信方式，采用 2 种线路纠错编码。其中，有线、无线通信采用一种编码

收稿日期：2016-07-14；修回日期：2016-08-20
作者简介：姜广顺(1967—)，男，山东人，硕士，工程师，从事装备维修和保障技术研究。

方式，音频通信采用另一种编码方式，2 种编码方式均为循环编码。在录取装备不同工作状态下的数据信息的基础上，查找数据流向，确定编码器的入口、出口，通过大量数据分析和理论计算，获取了系统的编(解)码方案。经过样机的对接试验，验证了编码方案的正确性。

在有线、无线通信方式下，进行(31, 25)系统循环编码，生成多项式 $g(x)=x^6+x^2+x+1$，形成 31 位码字，加入 1 个逻辑间隔(低电平)后，生成 32 位信息码字。利用该编码方式，数字信息处理分系统可检测到 2 个并纠正 1 个误码。

采用音频通信方式时，进行(38, 25)系统循环编码，生成多项式 $g(x)=x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^6+x^3+x+1$。利用这种编码方式，数字信息处理分系统能够检测不大于 5 个错误。当检测到错误时，输出错误指示信号。

2.2　数据结构

数据结构，即数据传输的帧组成结构，包括训练序列、时钟同步、帧同步、编码后的有效数据等信息，弄清帧结构是实现国产化遥码通信系统与原系统互通的必要条件。在缺乏参考资料的情况下，通过对装备采集数据的分析和深入挖掘，理清了原遥码通信系统数据的帧结构，通过样机的对接试验，验证了数据帧结构的正确性。其中，无线通道线路发送数据帧结构，见图 2。

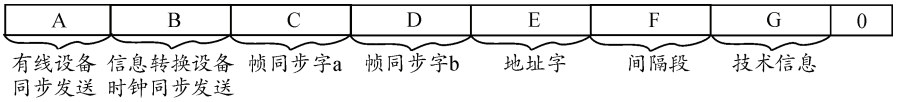

图 2　无线通道线路发送数据帧结构

A. 有线设备同步发送：“0111_0011”×12=96 位；

B. 信息转换设备时钟同步发送：“01”×8=16 位；

C. 帧同步字 a：0_00110_11101_01000_01001_01100_11111=31 位；

D. 帧同步字 b：00110_10010_00010_10=17 位；

E. 地址字：32 位；

F. 间隔段：128 个‘0’；

G. 技术信息：18 个字，(31, 25)的循环码，间隔位为‘0’，共 18×32=576 位。

2.3　调制、解调方式

原遥码通信系统主要采用频移键控(FSK)和四相相移键控(QPSK)2 种调制方式，国产化系统的调制方式要与原系统保持一致。通过大量测试，了解原系统调制方式的设计细节，并通过样机进行接收解调、验证，原遥码通信系统为时分工作模式，数据为瞬时、突发形式，而 QPSK 采用相干解调，需要快速恢复时钟，这就对载波的提取提出了更高的要求，国产化系统设计中充分利用原帧结构中的训练序列，有效地解决了这一问题。QPSK 调制和解调框图，分别见图 3、图 4。

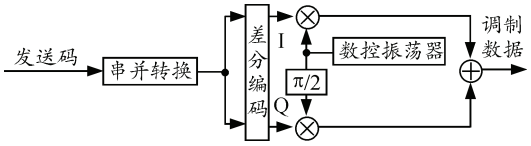

图 3　QPSK 调制

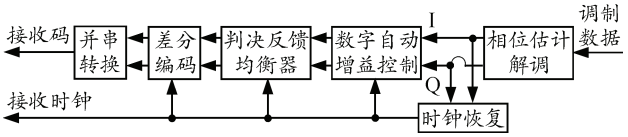

图 4　QPSK 解调

发送数据时，调制器将从信息转换装置传来的串行数据，经串并转换，输出 2 路并行数据(I 路和 Q 路)，为避免绝对 QPSK 调制方式带来的相位模糊问题，系统对 I、Q 2 条支路经差分编码单元将绝对码变换成相对码，以形成相对移相 QPSK 调制方式(即 DQPSK)。差分编码后的 2 路信号，分别与来自数控振荡器输出的 2 路正交载波相乘。2 路信号经过调制后，再合并相加，就得到四相移相键控信号，经 D/A 转换后送发送通道进行滤波和放大处理。

接收数据时，接收通道处理后的模拟调制信号经 A/D 转换成数字信号进入解调器，解调器从接收的信号中恢复出 2 路未判决的原始信号，然后根据恢复的数据时钟，经过数字自动增益控制、自适应判决反馈均衡器、差分解码、并串转换后，即完成整个解调过程。恢复出的解调数据即为接收码，它将与恢复出的接收时钟一同送到信息转换装置。接收时钟的下降沿应处于接收码元的正中央。

3　国产化遥码通信系统硬件设计

3.1　国产化遥码通信系统硬件组成

国产化遥码通信系统主站和从站分别由控制检查分系统、数字信息处理分系统、无线通信分系统、有线通信分系统、音频通信分系统、系统电源 6 部

分组成，系统功能组成框图，见图 5。

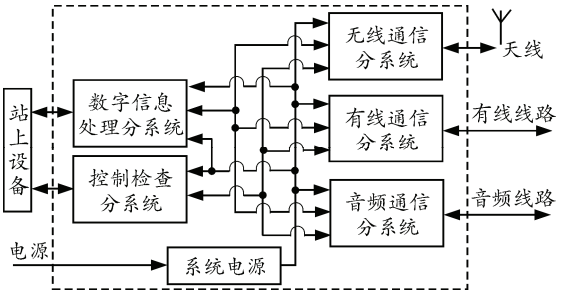

图 5　国产化遥码通信系统主(从)站功能组成

3.2　设计中解决的主要问题

1) 设计接口驱动电路。

遥码通信系统用于数字信息的正确传输，除了信息传输的正确性，还要保证数据接口信息交换的正确性。数字信息来源于专用计算机，接口为专用多路信息交换通道协议，接口控制信号多，时序要求严格，输入阻抗在 100 Ω 左右，要求信号在高电平 2.4 V 时，100 Ω 阻抗的驱动电流为 24 mA，接近数字逻辑芯片驱动的极限电流。为此，笔者设计了图 6 所示的接口驱动电路。

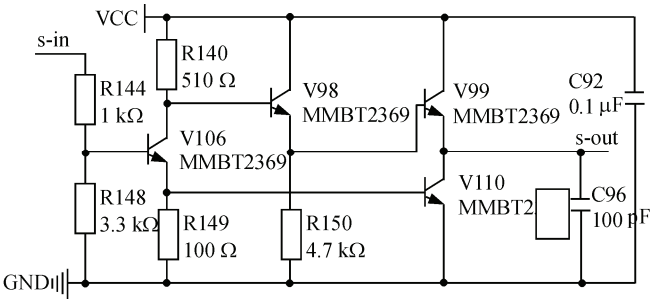

图 6　数字接口驱动电路原理

2) 研制数控振荡器。

国产化遥码通信系统中使用的数控振荡器原理框图，见图 7。

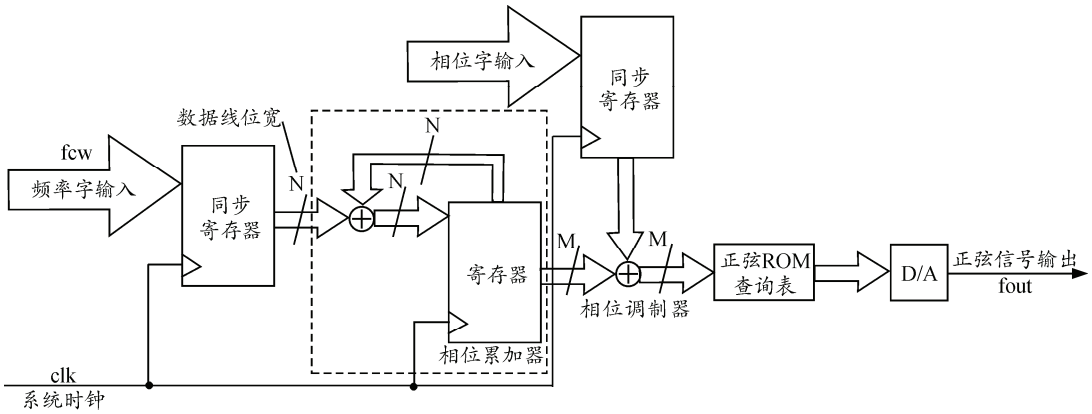

图 7　数控振荡器原理

将输入的频率控制字(fcw)进入累加器中进行相位累加，累加器的输出就是信号的当前相位。ROM 表中存储着不同相位时正弦信号所对应的幅度。将累加器的输出作为 ROM 表的地址进行查询，完成相位到幅度的转换即生成数字正弦信号，再经过 D/A 转换变成模拟正弦信号。

4　对比测试

在专用测试台上，对国产化遥码通信系统与原遥码通信系统进行了性能对比测试，输出功率、灵敏度、转入战斗状态时间等主要指标均优于原遥码通信系统。国产化系统与原系统的性能指标对比，见表 1。

表 1　国产化系统与原系统性能指标对比

序号	指标名称	原系统指标值	国产化系统指标值		
			主站	从站 1	从站 2
1	无线通信输出功率/dBm	≥51.8	52.5	53.0	52.4
2	无线通信灵敏度(Ⅰ波段)/dBm	≤−87 (≤15 μV)	−90.5	−89.0	−89.8
3	无线通信灵敏度(Ⅱ波段) /dBm	≤−84 (≤20 μV)	−90.2	−90.4	−90.3
4	音频通信发送功率/dBm	0～−4	−0.9	−0.8	−1.3
5	音频通信灵敏度/dBm	≤−26	−27.9	−27.8	−28.3
6	有线通信发送功率/dBm	≥0	0.5	1.1	0.4
7	有线通信灵敏度/dBm	≤−40	−45.5	−44.9	−45.6
8	转入战斗状态时间(自动功检)/s	≤40	＜1	＜1	＜1
9	转入战斗状态时间(不功检)/s	≤5	＜1	＜1	＜1
10	系统功耗/W	≤3 000	1 762.5	1 387.5	1 462.5

(下转第 16 页)