自主标准 RFID 信令的分析设计及实践*

李 军
（深圳市检验检疫科学研究院 深圳 518000）

摘 要：目前 RFID 技术已全面进入应用推广期，采用我国自主 GB 29768 标准和 GB 28925 标准技术的产品，也越来越广泛的应用于交通、物流、零售等领域，对于集成应用系统来说，除标准中定义的产品级符合性和性能测试项目以外，还需要进行系统级测试，例如通过信号流盘回放，分析信令数据和时序参数，用于故障定位和系统优化。使用模块化仪器对自主标准 RFID 信令进行分析设计以及实践。

关键词：射频识别；信令分析；信号流盘；软件无线电
中图分类号：TN98 **文献标识码**：A **国家标准学科分类代码**：510.4010

Design and practice of RFID signaling analysis

Li Jun
(Shenzhen Academy of Inspection and Quarantine, Shenzhen 518000, China)

Abstract: At present, RFID technology has fully entered the application promotion period, the products based on Chinese autonomous standard GB 29768 and GB 28925 have been widely used in traffic, logistics, retail and other fields more and more. In addition to the product-level conformance and performance testing defined in the standard, there is requirement for the system-level testing for the integrated application system, such as signal streaming and playback for signaling analysis of data and timing parameters, to help on trouble shooting and system optimization. This article will use the modular instrument to carry on the analysis design and the practice to the independent standard RFID signaling.

Keywords: RFID; signaling analysis; signal streaming; SDR

0 引 言

长期以来，RFID 关键技术专利基本掌握在美国、日本和欧洲等国家和地区的跨国公司中，形成了较强的专利保护布局，导致国内核心技术研发和产业发展一直都处于技术跟随阶段。为了满足国内 RFID 技术的应用和发展，国家标准委员会于 2010 年开始制定自主 RFID 标准。自此，自主标准 RFID 应用得到快速发展。但是，对于自主标准 RFID 信令的探测和分析，国内目前处于空白状态。本文使用模块化仪器对自主标准 RFID 信令进行分析和实践，主要面向于 RFID 读写器和标签通信过程中的信令数据，通过分析读写器和标签之间的信令收发序列，并且进行跟踪和测试，可以直观观察到读写器和标签间通信的时序，并能分析出产生问题的信令点，同时能在无需解析安全信息包的情况下，进行读写器和标签之间的安全分析和测试。

1 需求分析

RFID 信令分析需要解决的关键问题包括长时间的信令探测、跟踪和信令分析，以及进行序列自动分析和通信断点分析等。设计采用模块化仪器技术，解决传统仪器设备扩展性差，不能够支持自主标准 RFID 通信协议的问题，采用开放高速总线技术，解决长时间的信令探测、跟踪过程中的采集和存储的问题，采用数字信号处理技术，解决信令分析，序列自动分析和通信断点分析的问题。

2 系统设计

RFID 信令分析系统的设计应当按照标准化、模块化、层次化的体系结构进行。使用模块化仪器搭建 RFID 信令分析系统，主要由嵌入式主控模块、射频接收模块、

收稿日期：2017-04
* **基金项目**：国家质检总局科技计划项目(2015IK262、2015IK261)、深圳市科技计划项目(JCYJ20130101161330012)资助

FPGA信号处理模块和数据存储模块等组成。

在RFID产品进行无线通信的过程中，信令分析系统需要首先通过射频信号接收模块对空中信号进行接收和采集，然后根据不同的测试需求，对信令数据进行实时或者离线的分析。

2.1 信令分析

对于单品测试，可以启用基于FPGA的实时分析，对采集到的信号进行实时的数字信号处理，得出信令数据进行分析和验证。对于产品集群的测试，可以启用高速信号流盘模块，对采集到的信号进行高速的数据流盘和数据管理，以便后续进行离线分析。

在离线分析模式下，信令分析系统首先通过数据回放模块，对存储的数据进行重现，通过自动或者人工选择需要分析的信号片段，导入基于CPU的离线分析，对选定的信号进行离线的数字信号处理，得出信令数据进行分析和验证。

2.2 系统层次

RFID信令分析系统的总体结构分为设备层和应用层。

设备层是和硬件设备直接相关的部分，根据具体的功能需求，选取适合的模块化仪器构成，设备层也包括硬件设备的驱动和控制，以及信号处理算法等。应用层是和操作人员直接相关的部分，主要包括任务设置、信号和数据的选取、分析结果的显示和记录等。

设备层和应用层的主要接口包括从应用层到设备层的任务下达，以及从设备层到应用层的数据上传，任务和数据的传输都通过开放高速总线进行，以保证良好的吞吐量。

RFID信令分析系统设备层结构如图1所示，嵌入式主控模块、射频接收模块、FPGA信号处理模块和数据存储模块等硬件通过开放高速总线交换数据及命令。嵌入式主控模块用于测试流程的控制和信号的离线处理，射频接收模块、FPGA信号处理模块和数据存储模块用于信号的实时采集、存储和处理。其中，数字信号处理是整个RFID信令分析系统的核心，主要利用FPGA和CPU的强大处理能力，实现自主RFID标准的无线通信算法，如调制解调、编码解码、数据帧解析、协议状态分析等基础功能、设备层的各个功能模块由应用层进行统一的控制和调用。

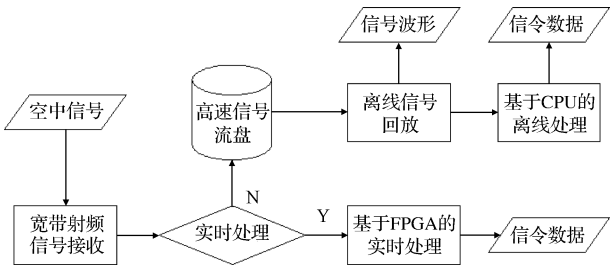

图1 设备层原理

测试过程中嵌入式主控模块接收应用层的用户任务，并发送命令给各个功能模块，射频接收模块从天线接收RFID读写器和标签通信过程中的空中射频信号，经过射频下变频后进行采样得到数字基带信号。如果任务设置为实时处理模式，将数字基带信号传送给FPGA信号处理模块，进行基于FPGA的实时处理，得到实时的信令数据，如果任务设置为离线处理模式，将数字基带信号传送给数据存储模块进行高速信号流盘。嵌入式主控模块能够对存储的信号可以进行离线信号回放，重现信号波形进行基于CPU的离线处理，得到离线的信令数据。

RFID信令分析系统应用层结构如图2所示，在硬件设备的驱动和控制，以及信号处理算法之上，应用层主要由用户的任务、设置和操作，数据的分析、显示和记录等模块组成，通过调用设备层的各个硬件模块实现具体的分析功能。虽然不同RFID无线通信协议的具体实现方式都不尽相同，但得益于软件无线电技术的高度灵活性，RFID信令分析系统的实现过程中可以进行层次化、模块化的封装，将不同RFID产品的信令分析功能很好的整合在一起。

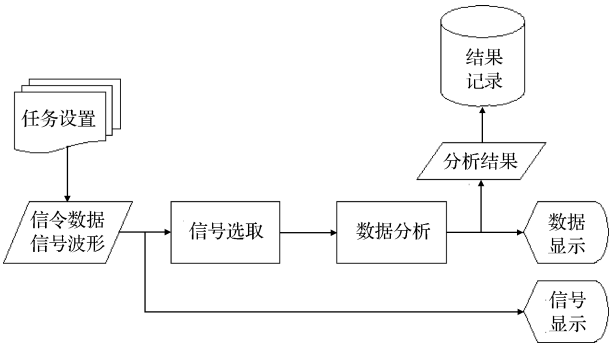

图2 应用层原理

测试过程中用户通过图形化界面对采集分析任务进行设置，例如接收信号的信道，采集时间的长度，处理模式等，设备层根据用户任务返回对应的信号波形或信令数据。对于实时处理模式，设备层直接返回实时的信令数据，对于离线处理模式，设备层返回离线的信号波形，通过自动或者人工选择需要分析的信号片段，得到离线的信令数据。信号波形和信令数据分别传送给对应的显示模块进行波形和数据的显示。信令数据同时也传送给数据分析模块进行更多的协议分析，例如协议状态、通信时序等，分析结果和原始数据都可以通过结果记录模块进行记录。

3 测试实践

基于以上系统设计，对我国自主GB 29768标准和GB 28925标准的RFID信令进行了测试实践。

RFID信令分析系统用户界面首先对离线信号回放的波形及相关的辅助信息进行显示，由于高速信号流盘过程中储存的数据量很大，并且其中对于测试有意义的信号可

能只占很小的一部分，所以离线信号回放过程中，需要将信号的缩略图进行显示，图表的时间轴为 s 级，用于用户人工判定其中是否包含有效的 RFID 无线通信信号，以及有效信号所在的大概时间。用户可以根据缩略图对显示的信号进行缩放，以显示信号的波形细节，图表的时间轴为 ms 级。离线回放的信号中同时包含了来自读写器和来自标签的信号，为了便于用户查看和后续的信号选取，在信号显示模块中还集成了信号识别功能，主要根据信号的特征量判定数据帧是读写器信号还是标签信号，并采用不同的信号标记进行区分。

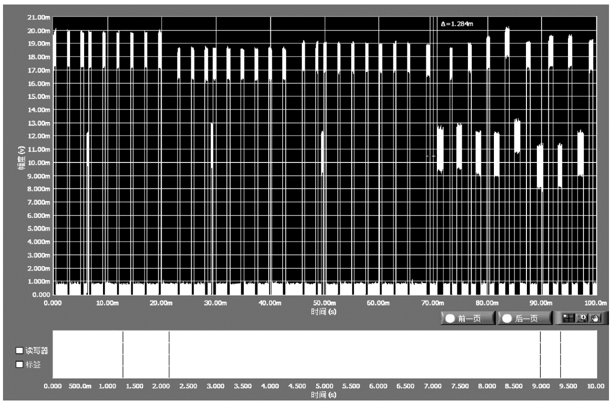

图 3　信令分析示例

信令分析结果的显示主要采用数据流和状态图两种方式，其中数据流如图 4 所示，主要以时间为依据显示 RFID 无线通信过程中读写器和标签之间的信令数据，显示图表上包括读写器到标签，和标签到读写器两类数据，用户可以点击其中的某个步骤以显示通信程中的具体数据，例如协议状态、信令名称、信令数据、通信时序等信息。

图 4　数据流分析示例

信令数据可以进一步进行信令流程的分析，明确被分析的数据属于何种流程，例如查询流程，防碰撞流程或读写流程等，根据流程的种类，分析读写器和标签是否在特定的时刻返回了正确的信令，对于通信失败的流程，再进行通信断点分析，确定读写器和标签之间是因为哪一个设备，在哪一步骤返回了错误的信令，或者没有返回信令。由于 RFID 无线通信协议中的安全算法需要专用安全芯片才能实现，信令分析系统还可以通过信令流程的分析，实现在不解析安全信息包的情况下，进行读写器和标签之间的安全符合性分析和验证。

信令流程分析完成后，根据协议标准规定的状态机，可以对流程中的各个步骤进行协议状态的分析，确认读写器的标签是否在特定的时刻处于正确的状态。进一步的，还可以对信令数据的格式和其中的参数数值进行分析，以判断正确与否。协议状态如图 5 所示，主要以协议状态为依据显示 RFID 无线通信过程中读写器和标签之间的信令数据，显示图表上包括读写器和标签通信过程中经过的所有状态，用户可以点击其中的某个状态以显示状态跳转过程中的具体数据，例如信令名称、信令数据、通信时序等信息。

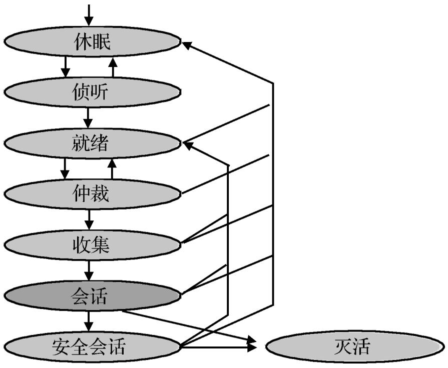

图 5　协议状态分析示例

4　结　论

目前我国 RFID 技术已进入快速发展的应用推广期，因此设计实现具有性能先进，功能强大，支持自主标准 RFID 的信令分析系统，对于满足国内 RFID 无线通信市场所需，推动自主标准 RFID 技术体系具有重要的意义。我院也将继续建立 RFID 标准验证测试平台，加强通信信令的探测、验证和分析能力，重点包括通信故障点的分析研究，以及空中接口安全符合性验证和分析研究，为自主标准 RFID 的加大应用推广提供支持。

参 考 文 献

[1]　GB/T 29768 信息技术射频识别 800/900 MHz 空中接口协议[S]. 2013.

[2]　GB/T 28925 信息技术射频识别 2.45 GHz 空中接口协议[S]. 2012.

[3]　GB/T 28926 信息技术射频识别 2.45 GHz 空中接口符合性测试方法[S]. 北京：人民邮电出版社，2012.

[4]　刘岩. RFID 通信测试技术及应用[M]. 北京：人民邮电出版社，2010.

[5]　李军，何婷婷，陈柯. 超高频 RFID 标准和测试技术演进[J]. 国外电子测量技术，2015，34(9)：13-16.

[6]　陈柯，邵晖，何婷婷. 射频识别(RFID)系统构架和持续改善[J]. 国外电子测量技术，2015，34(4)：5-9.

[7]　陈柯，何婷婷. 基于软件无线电技术实现 RFID 全程

测试 [J]. 卡技术与安全，2009(5).
[8] National Instruments. Advanced RFID Measurements: Basic Theory to Protocol Conformance Test[R]. http://zone.ni.com/devzone/cda/tut/p/id/6645.
[9] National Instruments. RFID Testing [R]. http://www.ni.com/automatedtest/rfid.htm.
[10] Daniel M. Dobkin. The RF in RFID: Passive UHF RFID in Practice [M]. Newnes, September, 2007.

作 者 简 介

李军，1975 年出生，高级工程师。主要研究方向为物联网技术与应用。
E-mail:54678872@qq.com

Pickering Interfaces 推出新款 4 槽 USB/LXI 模块化机箱

小巧轻便，非常适合小规格应用

近日，Pickering Interfaces 作为业内领先的模块化信号开关和电子测试与验证仿真的供应商，宣布推出新款 4 槽 USB/LXI 模块化机箱。

该新款 4 槽模块化机箱(型号 60-105)延续了 Pickering 2 槽 USB/LXI 模块化机箱(型号 60-104)外形小巧轻便的优点，非常适用于便携式、台式以及一些空间有限的应用。这款机箱设计为桌面或机架式安装，并且具有可通过 USB 或 LXI 以太网进行远程控制的特点。通过网络实现远程控制使得测试系统可以在离目标设备尽可能近的位置进行开关操作。

新款 4 槽机箱内部可安装 1～4 个 Pickering 3U PXI 模块。可构建多达 2 208 个交叉点的开关矩阵或多达 72 通道的程控电阻/传感器仿真系统。

该款新机箱兼容 USB 3 并且完全兼容 LXI 接口。这些通信标准使得该款机箱能够通过大多数支持 HTML5 的个人计算机和平板电脑上的标准接口进行直接控制。凭借这种实用性的优点，该款机箱能够在模块化测试和测量市场中广泛地迎合各类应用的要求。

Pickering 承诺所有产品都包含标准的 3 年质保以及长期的产品支持服务。更多相关详情可前往官方网站：www.pickeringtest.com 进行查阅了解。