使用无线 - Scada 系统的远程数据采集

摘要

在本文中，我们开发了一个集成的无线 SCADA 系统，用于实时监测和访问远处的设备参数，如温度，压力，湿度的性能。为此，我们使用了基于 GPRS 技术的现有移动网络基础设施。监控和数据采集（SCADA）是一个不断发展和研究的领域。这个项目研究设计了一个可以通过基本的编程，插入相关的外围设备，并且兼容许多不同的 SCADA 应用程序的低成本设备。在一些昂贵的 SCADA 应用中的大部分价格花在使用专用通信基础设施的。通过基础设施的应用，在降低成本的同时设备的通用性质将得到保证。

无线 SCADA 处理使用移动电话网络，特别是通用分组无线服务（GPRS）来创建廉价但适应性强且易于使用的 SCADA 设备和基础设施。组成设备的硬件组件相对简单，但是定制的编写软件使其可以在线升级，并且能够提供给定 SCADA 应用在任何非预定时间发送和接收控制和数据信号的能力。

GPRS 是一种基于分组的无线电服务，能够“始终开启”连接，消除重复和耗时的拨号连接。它还将提供超过 40 Kbps 的实际吞吐量，与优秀的陆线模拟调制解调器连接的速度差不多。

通过使用无线 SCADA 系统，可以从远处精准地记录约 30℃左右的温度数据。以类似的方式，电能表的读数可以读取 223 千瓦时（KWH）。

设计合理的 SCADA 系统通过取消人工访问每个站点进行检查，数据收集/记录或进行调整的方式节省时间和金钱。

1.引言

监控和数据采集（SCADA）是一个过程控制系统，使现场操作员能够监控和控制分布在各个远程站点的过程。设计合理的 SCADA 系统通过取消人工访问每个站点进行检查，数据收集/记录或进行调整的方式节省时间和金钱。

由计算机，控制器，仪器;执行器，网络和接口组成的监控和数据采集系统使得管理自动化工业过程的控制，并通过数据收集分析成为可能。它们适用于从配电系统，食品加工到设施安全报警等所有类型的行业。

监控和数据采集是指执行数据采集和监控控制的系统。移动监控和数据采集（称为移动 SCADA）是 SCADA 以移动电话网络为基础通信介质的应用。 GSM 是当今最流行的无线通信技术;在世界各地广泛应用于通过手机短信的传输数据[1]，[5]

通用分组无线服务（GPRS）由于提供了一种实时在线的互连而没有任何基于时间的收费而被选择作为特定的移动通信协议使用。 SMS 是一种全球公认的无线服务，能够在移动用户和外部系统（如电子邮件，寻呼和语音邮件系统）之间传输字母数字消息。它是一种存储和转发消息到移动端和从移动端发送消息的方式。[16]

SMS 的好处包括收信通知和警报，保证的消息传递，为简明的信息提供可靠和低成本的通信机制，筛选消息和返回呼叫增加了用户生产力[5]。

1.1 SCADA 系统的组件

SCADA 系统通常由四个组件组成：

主控单元 - 这是系统的核心，由操作员控制。

远程单元 - 此单元安装于实际监控过程的位置。 它收集要求的过程数据，并将其发送到主单元。

通讯模式 - 此单元在主机和远程机器之间传输信号/数据。 通信模式可以是有线，无线媒体，卫星等。

软件 - 软件是操作员和设备之间的接口。 它允许操作员可视化和控制过程的功能。

1.2 传感器：RTD 基础

电阻温度检测器（RTD）由金属（通常为铂）的线圈或膜制成。 当加热时，金属的电阻增加; 当冷却时，电阻减小。

3.电阻随温度变化

4.铂在 0℃下 100 欧姆

5.非常准确

6.非常稳定

1.2.1 RTD 的特性

R = R0（1 +αT0）

其中 R0 = 00 处的电阻

α=电阻温度系数

T0 =以摄氏度表示的温度

1.3 电能表计算

电表或电能表是测量供应到住宅，商业或机器或由其产生的电能的量的装置。电表上最常见的测量单位是千瓦时，等于 1 小时的负载 1 千瓦或 3,600,000 焦耳所使用的能量。一般，能量（E）等于功率（P）乘以时间（t）。为了确定以千瓦时为单位的 E，P 必须以千瓦表示，t 必须以小时表示。[8]

E = Pt

如果 P 和 t 没有以千瓦和小时分别指定，那么在确定 E 之前必须将它们转换为这些单位，以千瓦时为单位。

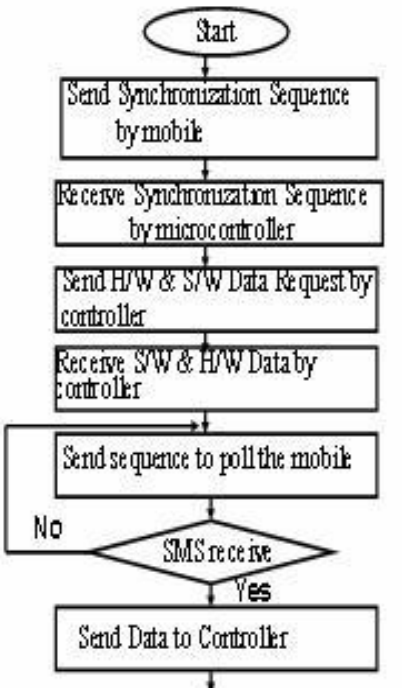
2.应用

应用的目的是在廉价无线通信的帮助下解决连续监测数据采集系统的问题的系统[12]，[14]

本文设计的远程监控系统的基本组件包括传感器，信号调理装置，AT90S8515 微控制器和手机。传感器，即 RTD 用于测量远程区域温度或能量计读数。基于微控制器的数据记录器完全取决于正在测量什么数据。 AT90S8515 是一款低功耗，高性能 CMOS 8 位微控制器，具有 8K 字节的系统内可编程闪存。微控制器使用 C 语言编程。[11]

关于无线通信。我使用 GSM 移动与 GPRS 服务。在这个项目中，诺基亚 3310 手机用于 GSM 通信。大多数诺基亚手机具有 F-Bus 连接，可用于将手机连接到微控制器。这个总线将允许我们发送和接收 SMS 消息[4]。

2.1 无线 SCADA 流程图



2.2 帧格式

总帧-98 字节（0-97）F 总线帧头（6 字节）

字节 0：F 总线帧 ID（0x1E）。 字节 1：目标地址（0x00）字节 2：源地址（0x0C）。

字节 3：消息类型 0x02（SMS 处理）。 字节 4 和 5：消息长度。

短消息帧头（18 字节）

字节 6 到 8：SMS 帧头的开始（0x00,0x01,0x00）

字节 9 到 11：发送 SMS 消息（0x01,0x02,0x00）

字节 12：短信中心号码长度。 0x0a 为 10 个字节长。

字节 13：SMSC 号码类型（0x81-unknown0x91-national

字节 14 到 23：短信中心电话号码（TPDU）传输协议数据单元（5 字节）

字节 24：消息类型（1-sms 提交，0-sms 提供）

字节 25：如果使用 SMS 提供和有效性指示器的消息参考

字节 26：协议 ID。 （0x00）

字节 27：数据编码方案。

字节 28：消息大小为十六进制的 0x22 或十进制的 34 字节长。

这是解压缩的消息的大小。

目的地电话号码（12 字节）

字节 29：目的地的号码长度。

字节 30：数字类型 0x91-international，0xa1-national

字节 31 到 40：（八位字节格式）目的地的电话号码

有效期（7 字节）

字节 41：有效期代码。 （0xFF）

字节 42 到 47：服务中心时间戳（0x00 ...。0x00）

SMS 消息（SMS-SUBMIT）（45 字节）

字节 48 到 92：短信包装成 7 位字符。

字节 93：始终为 0x00

F 总线帧结束（4 字节）

字节 94：分组序列号

字节 95：填充字节 - 字符串是旧的，需要是偶数

字节 96 和 97：奇偶校验和字节。

参考文献

1.Sungmo Jung, Jae-gu Song, Seoksoo Kim, “Design on SCADA Test-bed and Security Device,” International

Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 4, October, 2008

2. Sandip C.Patel, Pritimoy Sanyal ” Securing SCADA System” Information Management & Computer

Security Journal Volume: 16 Issue: 4 Page: 398 – 414 Year: 2008

3. Gumbo, S, Muyingi, H, “Development of a web based interface for remote monitoring of a Long-distance power transmission overhead line”, SATNAC 2007, Sugar Beach Resort, Mauritius,

ISBN 978 0 620 39351 5

4. http://www.embedtronics.com. online details of frame format of NOKIA

5. Surve, V, 2006, “A wireless Communication Device for Short Messages”, Masters Thesis, Available: www.certec.lth.se/doc/awireless.pdf .

6. Das, AN, Lewis, FL, Popa, DO, 2006, “Data-logging and Supervisory Control in Wireless Sensor

Networks,” Proceeding of the Seventh ACIS International Conference on Software Engineering,

Artificial Intelligence, networking, and Parallel/Distributed Computing (SNPD’06), Volume 00,

ISBN:0-7695-2611-X, pp 330- 338

7. Hildick-Smith, Andrew, “Security for Critical Infrastructure SCADA Systems,” (SANS Reading Room,

GSEC Practical Assignment, Version 1.4c, Option 1, February 2005),

http://www.sans.org/reading_room/whitepapers/warfare/1644.php

8. Carlson, Rolf E. and Jeffrey E. Dagle, Shabbir A. Shamsuddin, Robert P. Evans, “A Summary of

Control System Security Standards Activities in the Energy Sector,” Department of Energy Office of

Electricity Delivery and Energy Reliability,66 National SCADA Test Bed, October 2005,

http://www.sandia.gov/scada/documents/CISSWG_Report_1_Final.pdf

9. Technical Information Bulletin 04-1, Supervisory Control and Data Acquisition (SCADA) Systems, NCS TIB

04-1, Oct. 2004

10. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE

Dr. Aditya Goel & Ravi Shankar Mishra

International Journal of Engineering (IJE), Volume (3) : Issue (1) 65

Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002; receives the IEEE Communications

Society 2003 Best Tutorial Paper Award, April 2003.

11. Bement , Arden “Keynote Address at the NSF Workshop on Critical Infrastructure Protection for

SCADA & IT,” October 20, 2003 , http://www.nist.gov/speeches/bement_102003.htm .

12. McClanahan, R.H.,” The Benefits of Networked SCADA Systems Utilizing IP Enabled Networks", Proc. Of

IEEE Rural Electric Power Conference 5-7 May 2002 Pages: C5 - C5_7

13. Dagle, J.E.; Widergren, S.E.; Johnson, J.M.” Enhancing the security of supervisory control and data

acquisition (SCADA) systems: the lifeblood of modern energy infrastructures” Power Engineering

Society Winter Meeting, 2002. IEEE Volume 1, Issue , 2002 Page(s): 635 vol.1

14. J.E. Dagle (SM), S.E. Widergren (SM), and J.M. Johnson (M)” Enhancing the Security of Supervisory

Control and Data Acquisition (SCADA) Systems: The Lifeblood of Modern Energy Infrastructures”

Power Engineering Society Winter Meeting, 2002. IEEE Volume 1, Issue, 2002 Page(s): 635 vol.1

15. Stephen Beasley, Mr Choon Ng Dr Dario Toncich and Dr Andrew Dennison “Remote Diagnostics for Data

Acquisition Systems” white paper by Industrial Research Institute Swinburne Available online at

www.swinburne.edu.au/feis/iris/pdf/profiles/StephenBeasley.pdf

16. Taylor, K; “Mobile Monitoring and Control Infrastructure”, CSIRO Available online at

http://mobile.act.cmis.csiro.au