Integrating RFID readers for data acquisition in SCADA systems

Andrei Valeriu SMOLENIC, Vasile Gheorghită GĂITAN, Elisabeta TĂTULESCU
Mihai Florentin URSULEANU, Simona Anda GHERASIM
"Stefan cel Mare" University of Suceava
str.Universitătii nr.13, RO-720229 Suceava
andreis@eed.usv.ro

***Abstract* — with the rapid development of automation industry, the large companies realized the potential of SCADA software systems (Supervisory Control And Data Acquisition). Therefore, the use of these systems has become quite common. Also, the capability of devices to be used in SCADA systems came as a requirement for device manufacturers. This paper proposes a way of using RFID readers for data acquisition in a SCADA system.**

***Index Terms* — data acquisition, EDS, RFID, SCADA, tag**

I. INTRODUCTION

The rapid development of technology and the increasing competition in automation industry have determined the manufacturers of automation equipment to develop devices with increased complexity, greater capabilities and easier to operate.

According to [1], the SCADA (Supervisory Control And Data Acquisition) software systems are now common in the automation industry, being used to perform various tasks, ranging from different measurements (temperatures, pressures, etc.) to monitoring and controlling of systems from all industrial areas, some of them key areas in infrastructure. This paper proposes a way of using RFID readers for data acquisition in a SCADA system, extending the system's range of supported devices.

II. AN OVERVIEW OF RFID TECHNOLOGY

Over the past decade, a new inventory tracking technology emerged, called RFID (Radio Frequency Identification). The range of applications of this technology also increased rapidly, ranging from various inventorying processes, shipment tracking to secure building access and even securing the merchandise found in stores to prevent theft. This technology has a great potential and therefore this area is subjected to vast research.

In the RFID technology [2] there are two main components of an RFID system: the RFID reader connected to a computing device and the RFID tags.

Typically, an RFID tag is attached to an object and it provides an identity to that object.

An RFID tag is comprised of two components: a reduced size microchip and an integrated antenna. The microchip is used to store information about the object that the tag identifies. The information on the microchip contains a unique identifier for the object as well as different other characteristics that describe the object (last detection time, detection count, the antenna on which the tag has been detected – provided the reader has multiple antennas, etc.).

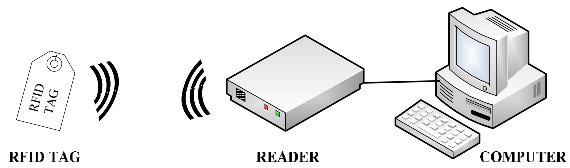

Fig. II-1: The main components of an RFID system

Currently there are two types of RFID tags known: active tags and passive tags. The passive tags are drawing power from the electromagnetic field emitted by the reader's antenna. The reader senses the tag because the tag alters the electromagnetic field. The active tags have their own power source, enabling them to emit an electromagnetic field of their own. Because of the built in power source, active tags are typically equipped with a more powerful microchip and a larger memory, but this also makes them more expensive than the passive tags.

When a tag is within the reading range of a reader, it is detected and its memory can be read, actually placing the object that the tag is representing in the reader's reading range. Some RFID readers can even detect if the object is stationary, approaching the antenna or moving away.

RFID tags operate in four frequency ranges: LF (Low Frequency), HF (High Frequency), UHF (Ultra High

Table II-1: The characteristics of radio frequencies [3]

	LF	**HF**	**UHF**	**Microwave**
Frequency range	125-135 kHz	13.56 MHz	400-960 MHz	2.45-5.8 GHz
Read range	<0.5 m (passive)	<1.0m (passive)	<10m (passive), >10m (semi-passive and active)	>100m (active)
Standards	ISO 11784/5, 14233, 18000-2	ISO 14443, 15693, 18000-3	ISO 18000-6/7, EPC Gen1 and 2	ISO 18000-4/5
Metal/fluid impact	Very low	Low	High	High
Data transfer rate	Low	Medium	High	High
Power and data transmission for passive tags	Inductive coupling	Inductive coupling	Propagation coupling	N/A
Typical industry	Farming, security, brewery	Pharmaceutical, health care	Manufacturing, logistics, construction	Army, shipping, airlines

Frequency) and SHF (Super High Frequency - Microwave) [3]. Table II-1 describes these frequency ranges.

Using the RFID technology brings numerous benefits:

- easier inventory tracking processes;
- lower production costs due to automating tasks of human operators;
- easier shipment tracking;
- reducing theft and many more.

III. AN OVERVIEW OF THE TARGET SCADA SISTEM

The target SCADA system was proposed and by [4]. The minimum requirements on which this model was built are:

- *to be a SCADA oriented application, able to acquire process data;*
- *to support a wide range of heterogeneous systems;*
- *to be scalable;*
- *to have real time characteristics;*
- *to use existing technologies and to be able to easily adapt to new technologies.*

This SCADA software system was designed based on the server-client paradigm. The *server* and *client* entities are communicating through a software middleware bus, which is responsible for carrying the data through the network, between server and clients. The server and client applications can coexist on the same computing system, they can be on different computing systems in the same network or they can be on different computing systems connected through the Internet.

The server is responsible for acquiring process data (temperatures, pressures, etc.) and making this data available to client applications. Both client and server applications of this SCADA system are built around the OPC specifications in order seamlessly acquire data from heterogeneous devices. Because the objective of this paper is to present a way to acquire data from an RFID reader through a SCADA system and knowing that the server application is responsible for acquiring data, a brief server description is necessary and is presented below.

The server is designed to be a modular application and is organized on three layers:

- the acquisition modules layer;
- the communication component layer;
- the data server layer.

The acquisition modules layer is actually a set of DLL libraries (Dynamic Link Library). Each DLL library acts as a driver for a certain type of device (device configuration, data acquisition, error detection, etc.). All DLL libraries are communicating with the upper layer (the communication component) by exposing the same set of functions. Because of this particularity, adding a new acquisition module does not imply rewriting the communication component, but simply implementing the driver and allowing access to the device's functionality through that specific set of functions.

The communication component manages the acquisition modules, stores de data acquired from devices in a buffer memory and exposes that data to the data server layer.

The data server layer handles the data received from the communication component by creating and managing OPC DCOM objects. It also provides a graphical user interface and ensures communications through the middleware bus with the client applications.

The SCADA system's architecture and dataflow is presented in Fig. III-1. The acquisition modules acquire data from the devices, they send that data to the communication component where the data is stored in the mentioned buffer memory, which is called the Object Dictionary.

The client applications connect to the data server and they gain access to different items (the data acquired from the devices). A client application can create groups with some of the items and set a refresh rate for the items in the group. On each refresh time, the new values are retrieved by the server from the communication component's buffer memory and sent to the client application.

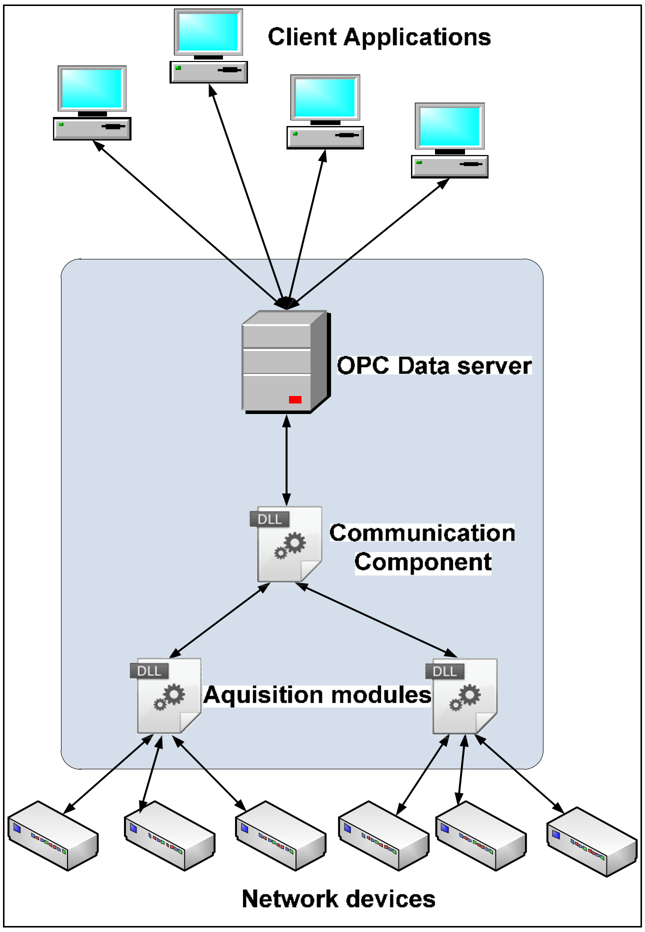

Fig. III-1: The architecture of the SCADA system

To be able to interact with the various devices, the server needs to know the structure of the data received from the devices as well as the commands required to interact with the devices (to retrieve the data, to store the data, etc.). Thus, every type of device is described using an EDS file (Electronic Data Sheet). The EDS file is comprised of the following sections:

- [FileInfo] – this section describes the file itself (name, version, description, file creation date, etc.);
- [DeviceInfo] – this section describes the device (manufacturer, name, serial number, etc.);
- [PdoObject] – the device's PDO objects (Process Data Object). These objects are in turn described through various parameters such as the object's name, access type, default value, description, stored data

type, etc.

- [SdoObject] – the device's SDO objects (Service Data Object);
- [History] – this section describes how the device's history log can be downloaded (if the device is able to provide a history log);
- [Communication] – this section describes the commands used to communicate with the device.

These EDS files are interpreted by both communication component and acquisition modules. The communication component interprets the EDS files in order to build the object dictionary. The acquisition modules are interpreting the EDS files to read the commands used for reading/writing data and passing that data to the communication component.

IV. THE RFID ACQUISITION MODULE

This acquisition module has been developed for the *Alien ALR-9900+ RFID reader* [5], built by *Alien Technology*. An image of the reader is presented in Fig. IV-1.

Fig. IV-1: The ALIEN ALR-9900+ RFID reader

The main technical specifications of this device are the following:

- it operates in the UHF 902 MHz - 928 MHz frequency range;
- it supports any tag compatible with the RFID EPC Class 1 Gen 2 tag protocol, standard ISO 18000-6c;
- 50 transmission channels with a channel spacing of 500 KHz;
- it can communicate on the RS-232 (DB-9 F) interface or on the LAN TCP/IP (RJ-45) interface;
- it can support up to 4 TNC monostatic antennas in circular or linear polarization;
- it can store up to 2500 tag records in a non-volatile memory in the event of a power loss;
- in autonomous mode it can collect up to 6000 tag records even if the LAN connection is lost, the records being available for download upon reconnection.

The next step in the developing of this acquisition module was the describing of the reader in an EDS file. The relevant section from the EDS file is the [PdoObject] section and is presented below:

```
[PdoObject]
[2000]
ObjectName = RFIDTag
AccesType = rw
[2000sub0]
Description  = NumberOfMembers
DefaultValue = 4
[2000sub1]
Description  = NUMAR_OF_TAGS
Type  = UNSIGNED8
[2000sub2]
Description  = TAG_1
Type  = STRING[20]
[2000sub3]
Description  = TAG_2
Type  = STRING[20]
[2000sub4]
Description  = TAG_3
Type  = STRING[20]
```

The EDS file describes a number of 3 RFID tags, specifying for each tag a name under which the tag will be seen in the server and a data type stored by the object, in our case `STRING[20]` will hold the tag's serial number in plain text. It can be observed that these EDS files can describe a static number of objects. This fact can be considered a problem because, in general, the RFID readers can have in their reading rang a variable number of tags.

A solution to this problem would be to describe in the EDS file the maximum number of tags (with blank default values) that the reader can provide at once. In this case, during the acquisition process, the acquisition module would modify a number of objects in the server equal to the number of tags in range of the reader, leaving the rest of the object to their default blank value.

This approach determines the server to allocate memory for all the objects described in the EDS file, even though the most of them will have the default blank value. Therefore the current approach is not advisable because our reader can provide a list of up to 6000 tag records. It would be a waste of memory on the server if we allocate memory for 6000 tag records if there are only 5 tags in the reader's reading range.

For that reason we chose to dynamically create the objects in the server as we are receiving the tag list from the reader, divided into memory blocks. Each memory block is independently analyzed. By doing this we don't occupy the server's memory with unusable objects. The tag list received from the reader is ASCII encoded and is comprised of tag records and the delimiters between them. This format easily allows us to navigate through the list and extract each tag record.

Because of the fact that RFID tags can have a wide range of uses, their memory can used in many ways, organized by any standard to hold meaning for its user.

EDS files were also used to describe the various memory organizations, using a single EDS file for each type of organization. In order to be able to link an EDS file to a type of memory organizations we used an identifier placed at the beginning of the tag's memory.

Judging from the point of view of a tag's flexible memory organization, we could consider an RFID tag as a dynamic acquisition device with an indefinite number of inputs and outputs, limited only by the tag's memory size.

V. CONCLUSION

Thus, data can be acquired from RFID readers and made available to a multitude of client applications within a SCADA system.

Furthermore, using RFID readers adds dynamism in SCADA systems from two points of view:

1. the number of tags located in a reader's reading range determines a dynamic number of acquisition devices connected to the SCADA system;
2. the dynamic number of inputs/outputs that can be defined within a tag's memory.

ACKNOWLEDGMENTS

This paper was supported by the project "Improvement of the doctoral studies quality in engineering science for development of the knowledge based society-QDOC" contract no. POSDRU/107/1.5/S/78534, project co-funded by the European Social Fund through the Sectorial Operational Program Human Resources 2007-2013.

REFERENCES

[1] X. Hong and W. Jianhua, "Using standard components in automation industry: A study on OPC Specification," *Computer Standards & Interfaces 28,* pp. 386-395, 2006.

[2] X. Zhu, S. K. Mukhopadhyay and H. Kurata, "A review of RFID technology and its managerial applications in different industries," *Journal of Engineering and Technology Management 29,* pp. 152-167, 2012.

[3] N. Li and B. Becerik-Gerber, "Performance-based evaluation of RFID-based indoor location sensing solutions for the built environment," *Advanced Engineering Informatics 25,* pp. 535-546, 2011.

[4] N.-C. GAITAN, V. G. GAITAN, S. G. PENTIUC, I. UNGUREAN and E. DODIU, "Middleware Based Model of Heterogeneous Systems for SCADA Distributed Applications," *Advances in Electrical and Computer Engineering,* vol. 10, no. 2, pp. 121-124, 2010.

[5] Alien Technology, "ALR-9900+ Enterprise RFID Reader," 9 January 2012. [Online]. Available: http://www.alientechnology.com/docs/products/Alien-Technology-ALR-9900-Enterprise-RFID-Reader.pdf.