NFC LIKE WIRELESS TECHNOLOGY FOR MONITORING PURPOSES IN SCIENTIFIC/INDUSTRIAL FACILITIES*

I. Badillo#, M. Eguiraun, ESS-Bilbao, Spain
J. Jugo, University of the Basque Country, Spain

Abstract

Wireless technologies are becoming more and more used in large industrial and scientific facilities like particle accelerators for facilitating the monitoring and indeed sensing in these kind of large environments. Cabled equipment means little flexibility in placement and is very expensive in both money and effort whenever reorganization or new installation is needed. So, when cabling is not really needed for performance reasons wireless monitoring and control is a good option, due to the speed of implementation. There are several wireless flavors to choose, as Bluetooth, Zigbee, WiFi, etc. depending on the requirements of each specific application. In this work a wireless monitoring system for EPICS is presented. The desired control system variables are acquired over the network and published in a mobile device, allowing the operator to check process variables everywhere the signal spreads. In this approach, a Python based server will be continuously getting EPICS Process Variables via Channel Access protocol and sending them through a WiFi standard 802.11 network using ICE middleware. ICE is a toolkit oriented to build distributed applications. Finally, the mobile device will read the data and show it to the operator. The security of the communication can be improved by means of a weak wireless signal, following the same idea as in NFC, but for more large distances. With this approach, local monitoring and control applications, as for example a vacuum control system for several pumps, are currently implemented.

INTRODUCTION

Reliable, fast and secure communications must be assured in every place of a large scientific facility, even more when large amount of data is involved due to the rapid development of computing and electronics devices. Cables are often irreplaceable, but when they are not really needed for performance reasons, wireless is a suitable option for monitoring and control due to the numerous advantages it offers: flexibility, mobility, scalability, reduced costs and ease of maintenance.

Different wireless solutions can be found in the market. The most widely used band for industrial and scientific purposes is the ISM band. Inside this, ZigBee [1], Bluetooth [2] and WiFi can be found. The EEE 802.11 standard for WLAN, WiFi, is a very flexible technology, easy to implement, cheap and which provides a wide bandwidth. For these reasons, it has been implemented in large-scale systems, as presented in [3].

However, the radio waves used in wireless networks create a risk where the network can be hacked, making system vulnerable to threats as denial of service, spoofing or eavesdropping. These issues make mandatory the implementation of security mechanisms to minimize this drawback in industrial uses as SSL/TLS protocols and a proper architecture. In [4] an improved security mechanism is studied.

The goal of the present work is to build a secure and reliable human machine interface system for data monitoring purposes in a large scientific facility, based on a idea similar to Near Field Communication (NFC) but adapted to industrial needs. NFC offers a great security against external attacks since the signal makes physically inaccessible outside the range of transmission, so data exchange can only be made inside a limited radius.

The main disadvantage of this protocol for the present goal, is that the transmission distance, 4 cm or less [5], is insufficient for monitoring and control purposes.

In consequence, the proposed approach uses a limited field communication scheme, with WiFi technology and limiting the signal power to avoid external intrusions depending on the particular characteristics of each application.

In the presented schema, a distributed environment based on a TCP/IP network is considered, where an Experimental and Industrial Control System (EPICS) control network is implemented, [6]. The system sends the desired data over the WiFi network and publishes it in an Android based mobile device, which must be located inside the wireless physical transmission range. Two-way communication will allow not only monitoring, but also changing signal values, for example to turn on/of a certain device.

The idea has been implemented for monitoring the vacuum control system of a negative ion source.

PROPOSED APPROACH

When designing a wireless communication system, security becomes critical, even more when talking about large scientific facilities. In these environments, such as ion sources and particle accelerators, intrusions may result in harmful or even disastrous situations due to the large amount of power involved in equipment consumption. In order to avoid undesired failures or data losses, developers of wireless standards incorporate a large variety of security related features in the protocols. Two of the most commonly used tools is message encryption and node verification. This is used in order to maintain

*Work funded by ESS Bilbao Consortium

#ibadillo@essbilbao.org

data integrity, prevent interception of the transmitted data between nodes of the network and avoid spoofing.

Another way to provide security to a wireless network, related to its architecture, is to adjust the transmit-power level to control signal spillage beyond the plant walls. If the radio signal is "invisible" beyond the limits of the facility, it becomes very difficult to steal or intercept the signal. That means a physical security against attacks, independently from the software security mechanism that will be implemented.

This idea is represented in Figure 1, where the mobile device located outside the transmission range cannot reach the wireless signal, therefore it is impossible to access information. It also allows to spread signals only in certain areas of the facility depending on the authorization level. So, a limited field communication approach can lead to a secure installation, limiting the transmission power accordingly to the characteristics of each area.

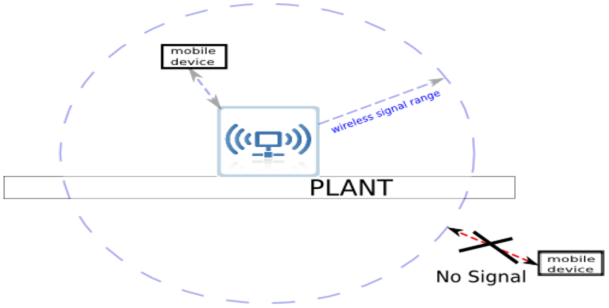


Figure 1: Security based on adjusting transmit-power level.

PROPOSED APPROACH IMPLEMENTATION

Large scientific facilities are complex distributed systems where important amounts of data must be processed and different control devices must be integrated. In this context, as every element might have independent behavior, a middleware distributing messages, commands signals and/or requirements over the net and between elements can be very helpful.

Nowadays, a large number of scientific facilities are being built using EPICS as middleware layer. Its wide usage, makes this solution very scalable. In fact, many vendors incorporate EPICS drivers in their products. Moreover, if a custom device is needed, in house development is also possible. This is the main control system used in the present limited field communication application.

On the other hand, the reduction in production cost of electronic devices and new technologies during last years has open a new market for mobile devices, such as tablets. In a large facility, a small and light computing device, with resources for networking environment, can help the operator in a lot of ways in both the usual operation and maintenance tasks. In this sense, Android based tablet has been chosen as mobile monitoring device, since its popularity and availability of many IDE environments make easy the development of custom applications.

Finally, as no libraries of EPICS for Android are available (unlike for iOS[7]), the use of the ICE middleware [8] is needed to integrate such different environments. It provides libraries for many programming languages, but, in addition to this, network security issues are a key issue of its functionalities.

The main characteristics of these technologies are summarized in the following paragraphs:

- EPICS: It is a control solution based on middleware approach, oriented to distributed control systems. It is used worldwide to create soft real time control systems specially for large scientific facilities as particle accelerators and telescopes. EPICS can be defined as an architecture for building scalable control systems, a collection of tools and codes made collaboratively between major science labs and industry. It is free and reliable and it is being more and more chosen to implement control systems in strategical projects as ITER (International Thermonuclear Experimental Reactor) or ESS (European Spallation Source). That eases feedback between developers in order to improve it. As mentioned before, the proposed networked control system architecture is based on a TCP network due to its advantages in cost and easy integration. But this protocol has non-deterministic characteristics, which makes difficult its use in control systems. The use of EPICS minimizes these disadvantages. Several EPICS controllers (IOCs) are spread along the facility, associated to different devices: sensors, DAQ systems and so on. These IOCs communicate among themselves and share information (Process Variables or PVs) using a protocol called Channel Access (CA) over a TCP/IP standard network. There are several security related mechanisms in EPICS, from among which highlights the EPICS Gateway. It is both a CA server and client and allows to separate the EPICS network from the network it is accessing from.
- ICE (Internet Communications Engine): This is an object-oriented toolkit for building distributed applications, heir of CORBA. It allows to communicate two or more applications of very different nature (operative systems, programming languages...). ICE offers different solutions for security, as encrypted communications and authentication through SSL, which is supported in all of the ICE language bindings.
- Android: Android is a mobile operative system based upon a modified version of the Linux kernel. Since the computing power of the mobile devices is quickly increasing and the price is reducing, its usage is fast spreading in different fields as industrial and scientific facilities [9]. Android is one of the leading OS for this kind of devices and it is updating and

adding services day by day, offering to the developers a huge number of tools to create any types of applications. The monitoring application is developed on an Android platform.

Implemented Architecture

In the implemented schema, a Python based server is used as a "bridge" between EPICS and the Android mobile device. This server program acquires the EPICS Process Variables over the network using the EpicsCA library [10], which provides methods for reading/writing PVs from Python via CA protocol. Moreover, the program organizes the captured PVs in a proper structure to ensure a good throughput and initializes the ICE host application. It creates the ICE object that responds to the client requests.

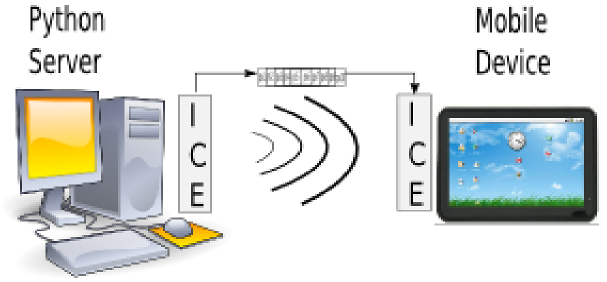


Figure 2: Client/Server communication using the ICE middleware.

Finally, the client is running in an Android mobile device. This application, written in Java, creates a proxy to connect to the object located in the server and invokes the needed operations to request the data. Once the data is obtained, the user interface displays the desired information to the operator. The Figure 2 shows a visual representation of the implemented schema.

SAMPLE APPLICATION: ISHN VACUUM SYSTEM MONITORING AND CONTROL

The presented application is intended to be used on a large scientific facility, to ease the task of the operators during normal operation and in maintenance stages. The main idea is to allow them to control and monitor the main variables of a vacuum system wherever they are inside the spread radius, depending on the transmission power. This fact allows to avoid the dependence of a central computer. Specifically, it has been designed to monitor the vacuum control system of the ISHN (Ion Source Hydrogen Negative) project at ESSBilbao, [11].

ISHN project consists of a Penning type ion source which will deliver up to 65mA of H− beam to a linear accelerator, which finishes generating neutrons by means of spallation process (currently under design). Apart from main devices for managing the ion source, for instance power supplies for plasma generation and hydrogen feed system, the vacuum system in considered a critical system of the project. For the ion source operation, a pressure value in the order of 10^{-6} mbar is required. Any failure could cause dramatic accident, due to the high voltage values needed for operation (several kilovolts), because a vacuum loss could cause high voltage breakdown.

In order to reach the desired vacuum level two mechanical and two turbo pumps are used. Their control system is isolated from the local control of the ion source, except for some interlock and emergency signals. There are managed by a PLC from Schneider, which reads all the signals involved in the operation of the pumps, such as rotation frequency, pressure level, status, etc. A Modbus TCP/IP server publishes all of these variables, and some of them can be accessed in both write and read mode.

An EPICS IOC accesses all of the data by Modbus TCP/IP calls [12], which acts as a wrapper for Twido communication. Even if Modbus communication is present, any call to vacuum system can only be done through EPICS, ensuring that capabilities offered by EPICS are always met.

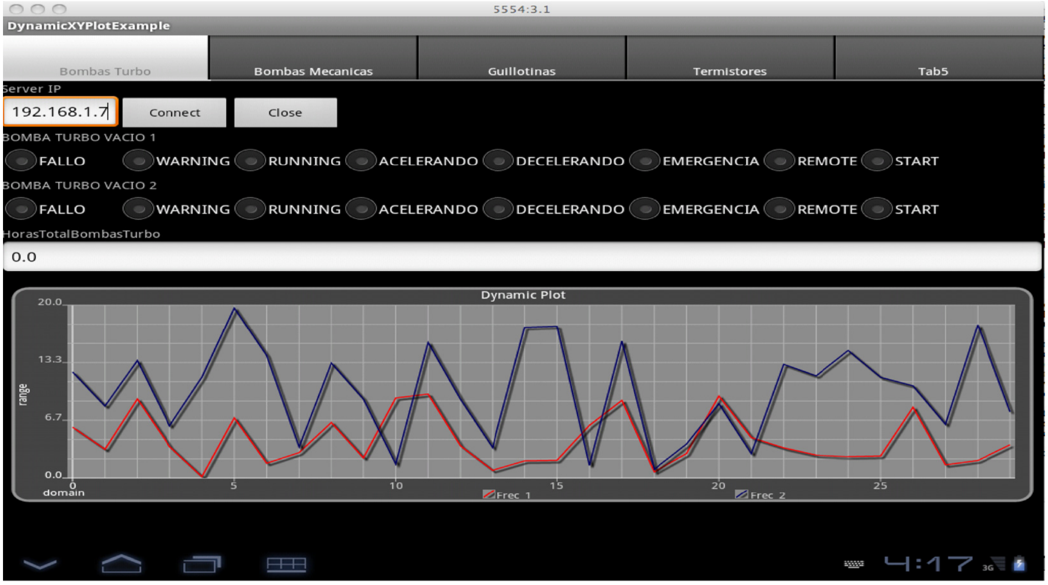
In such configuration, the devices controlled with EPICS are two mechanical pumps, two turbo pumps, a vacuum sensor and two vacuum gates.

The application for Android has been developed in Eclipse using the ADT (Android Development Tools) and tested on the emulator provided on the Android SDK [13]. The program has been written for the API Level 12 (Android 3.1), compatible with all the newer version and APIs. All the libraries used in the project are provided with the ADT, except the ICE specific ones and those used to build the XY plots. These last were imported from the "androidplot" project [14], which offers a pure Java API for creating dynamic and static charts within Android applications.

The GUI shows a text box where the user must enter the IP to connect to and a "connect" button. Most of the variables are booleans as on/off, alarm status etc., so they will be displayed using a widget that emulates a led, as shown in Figure 3. The analog signals, as rotation frequency of the turbo pumps or temperatures, are represented as a waveform chart which refreshes itself dynamically.

CONCLUSION

In this work, the use of wireless communications for monitoring and sensing in large industrial and scientific facilities has been discussed, proposing a limited field communication approach. In addition, a particular application of this technology has been presented. The advantages of wireless devices make this technology an interesting alternative to common wired and fixed monitoring stations. However, as long as wireless communications are involved, security becomes critical. Adjusting transmission power allows to spread the signal only in the desired radius, avoiding external attacks. A good mechanism limiting the transmission power depending on the application characteristics is also necessary.



Server IP
192.168.1.7

HorasTotalBombasTurbo
0.0

Figure 3: GUI of the Android application.

In particular, EPICS network distributed applications, which involve very heterogeneous environments, take advantage of the simplicity and capabilities of ICE toolkit and the versatility of Android based devices for LFC implementations.

The main purpose of the future work is to implement encrypted communications and authentication through SSL protocol. There is also projected to integrate the EPICS monitor system in a Python based server, to avoid polling in order to improve the overall throughput.

It is worth noting that the presented application will be implemented in the ESS Bilbao project for a real usage and it is intended to extend its monitoring and control tasks to several systems apart from the vacuum control system of ISHN.

REFERENCES

[1] W.-T. Sung and Y.-C. Hsu. Designing an industrial real-time measurement and monitoring system based on embedded system and ZigBee. EXPERT SYSTEMS WITH APPLICATIONS, 38(4):4522–4529, APR 2011.

[2] Bluetooth home page, http://www.bluetooth.com

[3] E. Witrant, A. D'Innocenzo, G. Sandou, F. Santucci, M. D. Di Benedetto, A. J. Isaksson, K. H. Johansson, S.-I. Niculescu, S. Olaru, E. Serra, S. Tennina, and U. Tiberi. Wireless ventilation control for large-scale systems: The mining industrial case. INTERNATIONAL JOURNAL OF ROBUST AND NONLINEAR CONTROL JAN 25 2010.

[4] R. Falk and H. J. Holf. *Industrial sensor network security architecture*. In *Emerging Security Information Systems and Technologies* (SECURWARE), 2010 *Fourth International Conference* on pages 97-102, july 2010

[5] E. Haselsteiner and K. Breitfuß. Security in near field communication (nfc). RFID sec, 2006.

[6] EPICS home page, http://aps.anl.gov/epics.com

[7] capod, EPICS CA libraries for iOS, sourceforge.net/projects/capod/?_test=beta

[8] Zeroc ice middleware, http://zeroc.com

[9] A system architecture for industrial application based on the Android Mobile OS, A. Sbaa, R. El Bejjet, H. Medromi

[10] Pyepics home page, http://cars9.uchicago.edu/software/pyton/pyepics3

[11] Ishn web, http://essbilbao.org

[12] EPICS Modbus, Mark Rivers, http://cars9.uchicago.edu/software/epics/modbus.html

[13] Android, http://developer.android.com

[14] Androidplot project, http://androidplot.com