ANDROID BASED MOBILE MONITORING SYSTEM FOR EPICS NETWORKS: VACUUM SYSTEM APPLICATION*

I. Badillo#, J. Jugo, Univ. Basque Country, Spain
I. Arreondo, M. Eguiraun, Jorge Feuchtwanger, G. Harper, ESS Bilbao, Spain

Abstract

When cabling is not really needed for performance reasons, wireless monitoring is a good choice for large scientific facilities like particle accelerators, due to the quick implementation. There are several wireless flavors: ZigBee, WiFi etc. depending on requirements of specific application. In this work, a wireless monitoring system for EPICS based on an Android device is presented. The task is to monitor the vacuum control system of ISHN project at ESSBilbao, where control system variables are acquired over the network and published in a mobile device. This allows the operator to check process variables everywhere the signal spreads. In this approach, a Python based server is continuously getting EPICS variables via CA protocol and sending them through a WiFi network using ICE middleware, a toolkit oriented to develop distributed applications. Finally, the mobile device reads and shows the data to the operator. The security of the communication is ensured by a limited WiFi signal spread, following the same idea as in NFC for larger distances. With this approach, local monitoring and control applications are easily implemented, useful in starting up and maintenance stages.

INTRODUCTION

In modern large scientific and industrial facilities, more and more information is needed due to the rising capabilities of the electronics and computing devices. For this reason, communications must be assured in every place of the facility. And this must be done in a reliable, fast and secure way. At this point cables seem to be the perfect solution. But when they are not really needed for performance reasons, wireless is a good option for monitoring and control. Wireless communications offer many advantages as reduced costs, mobility, scalability and ease of maintenance.

Several wireless solutions such as ZigBee [10],Bluetooth [3] or WiFi can be found on the market. The EEE 802.11 standard for WLAN, WiFi, is a very flexible technology, easy to implement, cheap and provides a wide bandwidth. For theese reasons, it has been implemented in large-scale systems, as presented in [11].

However, security can be a big drawback for this application in industrial uses. 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. Therefore, the architecture of the network becomes critical, in [8] an improved security mechanism is studied.

The goal of the present work is to build a secure and reliable machine to machine system for data monitoring purposes in a large scientific facility, based on a idea similar to Near Field Communication (NFC) but using WiFi standard technology. 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 disadvantage of this protocol is that the transmission distance, 4 cm or less [9], 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 depending on the particular characteristics of each application.

In the presented schema, a distributed environment based on a TCP network is considered, where a EPICS control network is implemented. The system acquires 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 allows not only monitoring, but also changing signal values, for example to turn on/of a certain device.

The idea has been implemented for monitoring a vacuum control system.

LIMITED FIELD COMMUNICATION APPROACH

Security is critical when designing a wireless communication system. Intrusions may result in harmful or even disastrous situations in large scientific facilities such as ion sources and particle accelerators, where many devices consume a large amount of power. In order to avoid undesired failures or data losses, developers of wireless standards incorporate a large variety of security related features in the protocols. One of the most commonly used tools is message encryption. This is used in order to maintain data integrity and prevent interception of the transmitted data between nodes of the network.

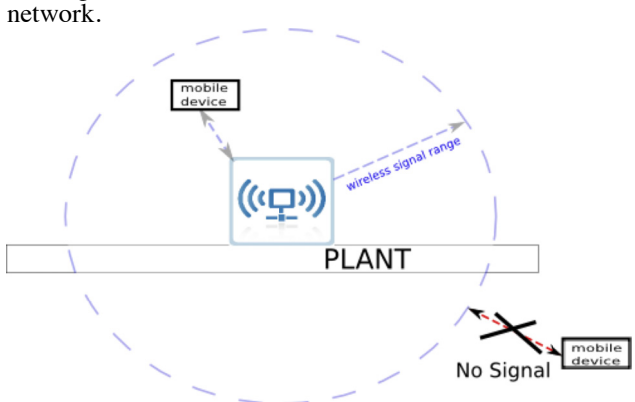

Figure 1: Security based on adjusting transmit-power level.

Another way to provide the security of a wireless network is adjusting 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

*Work funded by ESS Bilbao Consortium
#ibadillo@essbilbao.org

physical security against attacks. 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.

PROPOSED LFC APPROACH IMPLEMENTATION

Large scientific facilities are complex distributed systems were 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, most scientific facilities are being built using EPICS as middleware layer [4]. Its wide usage, makes this solution very scalable. In fact, many vendors incorporate EPICS drivers in their products. And, if a custom device is needed, in house development is also possible. This is the main control system used in the LFC 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 tablet devices. In a large facility, a small and light computing device, with resources for networking environment, can help in a lot of ways 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 toolkits environment make easy the development of custom applications.

Finally, with the aim of integrating EPICS and Android systems, ICE toolkit is used. Mainly, because it has 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 and a collaboration 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), what eases feedback between developers in order to improve it. As said before, the networked control system 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.

-ICE (Internet Communications Engine): This is an object-oriented toolkit for building distributed applications. It allows to communicate two or more applications of very different nature (operative systems, programming languages...) [7]. ICE offers different solutions for security, as encrypted communications and authentication through SSL, which is supported in all of the ICE language bindings.

-Android: The monitoring application is developed on an Android platform. 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. 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.

Implemented schema

The proposed LFC schema is the following: EPICS control system will be continuously publishing PVs in a network. A Python based server accesses this information through EpicsCA [6] by polling procedure. EpicsCA is a library that provides methods for reading from and writing to Epics Process Variables via the CA protocol from a Python program. Moreover, this program initializes the ICE host application, creating the object (communicator) for passing to the ICE client hosted on the Android device by mean of a WiFi network with limited transmission power, as well as organizing the EPICS PVs in a proper structure to ensure a good throughput.

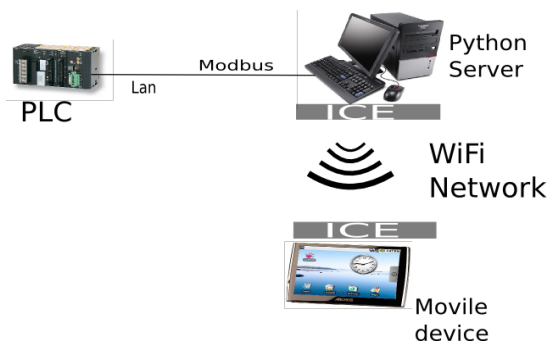

Figure 2: LFC system schema over the network.

Finally, the client is running in an Android mobile device. This application, written in Java, creates a proxy to connect to the server via ICE and calls the object (communicator) which is wanted to read/write. The user interface displays the desired information to the operator and allows to write to EPICS PVs easily using the touch screen. The figure 2 shows a visual representation of the implemented schema.

SAMPLE APPLICATION: 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, [5].

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 10–6mbar 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 control of the ion source, except for some interlock and emergency signals. There are managed by a Twido 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, 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 [1]. The program has been written for the API Level 7 (Android 2.1), compatible with all the newer version and APIs. All the libraries used in the project are provided with the ADT, except for the ICE specific ones and those used to build the XY plots. These last were imported from the "androidplot" project [2], which offers a pure Java API for creating dynamic and static charts within Android applications.

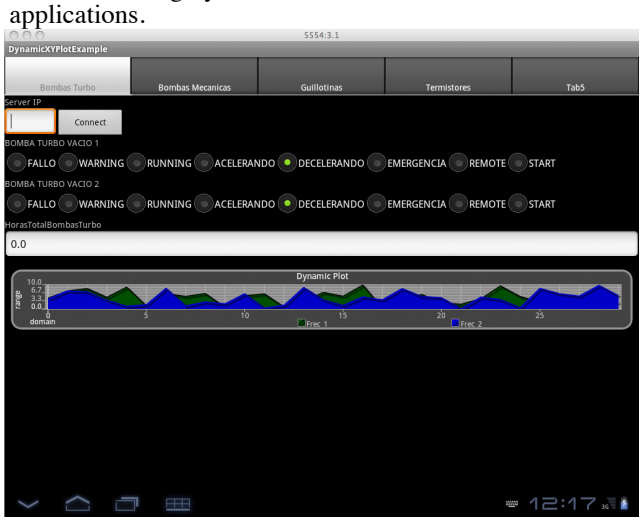

Figure 3: User interface of the Android application.

The GUI shows a text box where the user must enter the IP we want to connect to and a "connect" button. Most of the variables are booleans as on/off, alarm status etc., so they will be displayed as leds, as shown in figure 3. The rotation frequency of the turbo pumps representation is a waveform chart which refreshes dynamically.

CONCLUSION AND FUTURE WORK

In this work, the use of wireless communications for monitoring and sensing in large industrial and scientific facilities has been discussed, proposing the so called LFC 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.

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] Android, http://developer.android.com
[2] Androidplot project, http://androidplot.com
[3] Bluetooth home page, http://www.bluetooth.com
[4] EPICS home page, http://aps.anl.gov/epics.com
[5] Ishn web, http://essbilbao.org
[6] Pyepics home page, http://cars9.uchicago.edu/software/pyton/pyepics3
[7] Zeroc ice middleware, http://zeroc.com
[8] 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
[9] E. Haselsteiner and K. Breitfuß. Security in near field communication (nfc). RFID sec, 2006.
[10] W.-T. Sung and Y.-C. Hsu. Designing an industrial real- time measurement and monitoring system based on em- bedded system and ZigBee. EXPERT SYSTEMS WITH APPLICATIONS, 38(4):4522–4529, APR 2011.
[11] 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, 20(2, Sp. Iss. SI):226–251, JAN 25 2010.