

## Modern Human Machine Interface in Industrial Wireless Networks

Lysander Demaiter  
Electromechanical & Electrotechnical Engineering  
Ghent University  
Kortrijk, Belgium  
Lysander.Demaiter@UGent.be

Athar Qureshi & Predrag Rapajic  
Faculty of Engineering & Sciences  
University of Greenwich  
Chatham, United Kingdom  
qm05@gre.ac.uk;p.rapajic@gre.ac.uk

**Abstract**— This paper presents several existing experimental setups on latest industrial systems and provide comparison of advantages and disadvantages of different HMI implementation. It proposes a simple and low cost HMI system for automation by using remote software application. The method does not required specific software package from vendors, hence provide a low cost and easily available solutions for control. We have examined their switching on various wireless technologies including Bluetooth, Infrared, Wi-Fi and Cellular Mobile Systems. The presented HMI provide effective and inexpensive control of automation systems by using remote software packages on the mobile phone, tablet and laptop. This paper presents several experiments on HMIs. The first set of experiments are related existing HMI systems on latest Siemens TIA Portal software and hardware. The second set of experiments presents the developed method of HMI switching and control by using remote communication software; Vectir and Teamviewer over different industrial wireless technologies.

**Keywords**- Bluetooth, Infrared, HMI, Wifi, 2.5G, 3G and 4G

### I. INTRODUCTION

Automation is the use of control systems and information technology to reduce the need for manual work for the production of goods and services. Automation greatly decreases the need for human intervention and plays an important role in the fast growth of the world economy. Fundamentally, Industrial automation is incorporating many devices and tasks including programmable logic control (PLC), supervisory control and data acquisition (SCADA), human machine interface (HMI), Programing Device (PG/PC), Drives Control, embedded control, logic control, industrial landline and wireless communication etc. In precise words, Industrial Automation Engineering consists of combination of the various electrical, electronics, computer, communication and mechanical technologies. For many manufacturing companies, the labor cost is significantly high, which is one of their main reasons for investing in the automation for their production. A lower production cost allows companies to reduce the prices of their products and services. This enables them to compete with companies in low-wage countries and allows them to contribute to economic prosperity. There will be a significant increase in the use of automation systems in public places with HMI in order to perform daily routine tasks.

The previous research literature by researchers related to HMI for the control of local and remote robots was published in the paper [1]. The task interface and interaction HMI discussed in the paper [2]. Control by HMI is also presented in [3]. It has been found that in previous literature fever work has been performed to presents latest HMI application, practical setups and experiments, particularly in industrial automation. This paper gives an overview of various modern HMI systems that applied to Industrial Wireless Networks. Various wireless

technologies used for communication are presented in the experiments.

This research paper also presents a method of remote communication which only required a specific software package for remote control, and therefore provides a low cost solution. The performance was examined through the application of various wireless technologies including Bluetooth, Infrared, Wi-Fi and Cellular Mobile Systems. The presented methods are low cost solutions to control the system without the development of an additional software package. This research has developed practical set-ups and test-beds of HMI in industrial wireless communication systems and addresses various performance issues. HMI enable effective and inexpensive control of automation systems by using remote software packages on a mobile phone, tablet or laptop. With the recent emergence of cellular mobile devices for multi-tasking, everyone wants to have the control of their automation tasks on the cellular mobile device, i-Pod and laptops. In this paper, we presented a concept of the modern operating panel or SCADA/HMI for the control devices. We used commonly available web software applications that remotely control computers, these including Google, Teamviewer and Vectir. We demonstrated the control of automation systems in wireless networks by using these remote control software that eliminates the need for special software package for each automation system. For example, in Siemens Automation Systems we use WinCC software package for the operation of SCADA/HMI and devices. For Toshiba and Allen Bradley Automation systems, we would need a different package for the SCADA and HMI operations. In our proposed control method, we use remote control software packages that are easily available at low cost. It has used remote control

software applications and Mobile devices to obtain complete control of the PC/PG, connected to automation systems over various wireless communication technologies. We also discussed the benefits of remote control technologies in wireless networks. We have presented the wireless remote control via Bluetooth, Wifi and Cellular Mobile Phone [4][5][6]. We have shown that we can perform many switching by using remote control application. For example; one can obtain control over the automated task for home or office on their mobile phones and control the function. In industrial control, one can control the factory automation tasks remotely on their laptop or mobile phone. We can also efficiently perform configuration and commissioning tasks, route and remotely monitor faults by using the proposed system. Multi tasks can also perform to control remotely on multi web pages and we can also control the communication among various automation systems like communication between human body observations. We can install remote control applications to take full control of any remote computers over the mobile phone [7][8][9]. The presented concept has potential to develop applications and leads to machine to machine (M2M) systems that can be very useful in future communication, in nuclear submarine, smart homes, nuclear power station, space exploration, Mining, offshore drilling and many more applications. The presented research is beneficial solutions for the today's competitive communication product market as we need very little resources to implement these in industries. It can significantly reduce the cost of automatic control systems. Moreover, on multi computer nodes, we can address all of the issues related to safety, security and availability.

#### *Research Contributions:*

The research contributions of this paper are:

1. This research presents a brief overview of the commonly used industrial wireless standards.
2. We have presented the solutions to secure the industrial networks and provide brief overview of remote access.
3. This paper presents some of the existing HMI systems and present comparison between operating panel and web panel. The related experiments are also presented.
4. It proposes a concept of modern SCADA and HMI systems by using remote control software packages. It proposed a simple and low cost HMI system by using remote software applications on wireless systems. The proposed system can be operated over Bluetooth, Wi-Fi, 2G, 3G and 4G. The related practical experiments are carried out and explained.

The rest of paper consists of following: Section II briefly discusses Bluetooth technology. Section III represents Infrared Wireless technology. Section IV describes WiFi technology. Section V discusses the Cellular Mobile Systems (2G, 3G, 4G). Section VI is related to remote access and network security related issues. Chapter VII is related to the experimental setup and demonstration of the experiments. Chapter VIII is for the conclusion and future work.

## II. BLUETOOTH DATA COMMUNICATION

It is a wireless communication standard which operates on a very low electrical power. Bluetooth is a Wireless Personal Area Network (PAN). It consists of physical layer on IEEE 802.15.1 standards. The low power consumption makes it one of the very important green technologies. Bluetooth is an international wireless standard which provides wireless connectivity for various electronic devices and gadgets and plays important role in M2M communication. The use of this technology is in various fields including but not limited to mobile phone, wireless devices, smart home, retail, manufacturing, consumer electronics, personal computers, health, smart devices and fitness etc. It provides flexible development architecture for creating wireless applications. The Bluetooth core system consists of an RF transceiver, baseband, and protocol stack. It provides connections among equipment and exchange many data classes. It operates in the unlicensed 2.4 GHz (2400 - 2483.5 MHz) industrial scientific medical (ISM) frequency band. It has 79 RF channels (0-78) are spaced 1 MHz beginning at 2.402 GHz. Bluetooth uses frequency hopping spread spectrum multiplexing technique. The transmitted data are divided into packets and each packet is transmitted on one of the 79 designated Bluetooth channels to combat interference and fading. In Bluetooth wireless technology there are two supported modulation modes. First is the compulsory and less complex mode called Basic Rate, uses a shaped, binary FM modulation. There are also optional modes for Bluetooth for Enhanced Data Rate. It uses PSK modulation and has two variants:  $\pi/4$ -DQPSK and 8DPSK. The symbol rate of all modulation schemes is 1 Mbps. The achievable gross air data rate 1 Mbps for Basic Rate, 2 Mbps for  $\pi/4$ -DQPSK and 3 Mbps for 8DPSK. Time Division Duplex (TDD) scheme is used in both modes of full duplex transmission. Bluetooth2.0 supports data rates up to 2.1 Mbps with a range that depends on the power class of the product [10][11]. And it needs much less power than Wi-Fi, but the area covered and data rates are smaller. In most common implementations the range can be up to 1 m or 10m depending on the power class. It is a packet based protocol with a master-slave structure. In Bluetooth technology, one master can communicate with up to seven slaves in a Bluetooth network (Piconet), with the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5  $\mu$ s intervals. Two clock ticks make up a slot of 625 micro seconds; two slots make up a slot pair of 1250  $\mu$ s. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots; the slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long, but in all cases the master transmit will begin in even slots and the slave transmit in odd slots. The core architecture blocks consist of Channel Manager, L2CAP Resource Manager, Device Manager, Link Manager, Baseband Resource Manager, Link Controller and RF Block.

## III. INFRARED DATA COMMUNICATION

Infrared technology is always been very popular in remote controls of electronic gadgets. The very common example is the remote control of TV and Satellite receiver. Infrared technology allows devices to use short-range wireless signals

for communication. Using this technology we are not limited to house hold remote but also we can transfer files and other digital data, bi-directionally and it is similar to that used in consumer product remote control units. In our experiments of this paper, we used computer infrared network adapters both transmit and receive data through ports of a device. Infrared adapters are installed in many laptops and handheld personal devices. In Microsoft Windows, infrared connections can be created through the same method as other local area network connections. Infrared networks were designed to support direct two-computer connections only, created temporarily as the need arises. However, extensions to infrared technology also support more than two computers and semi-permanent networks. Wifi, Cellular Mobile and Bluetooth signal can penetrate through the wall but infrared network signals cannot penetrate walls. The communication range is 5 meters line of sight for infrared. Infrared technology used in local networks exists in three different forms:

IrDA-SIR (slow speed) infrared supporting data rates up to 115 Kbps. IrDA-MIR (medium speed) infrared supporting data rates up to 1.15 Mbps. IrDA-FIR (fast speed) infrared supporting data rates up to 4 Mbps. Infrared (IR) light is the electromagnetic radiation with longer wavelengths than those of visible light, extending from the nominal red edge of the visible spectrum at 700 nanometers (nm) to 1 mm. This range of wavelengths corresponds to a frequency range of approximately 430 THz down to 300 GHz. Most of the thermal radiation emitted by objects near room temperature is infrared. Slightly more than half of the total energy from the Sun was eventually found to arrive on Earth in the form of infrared. The key component of an infrared system is an infrared LED (Light Emitting Diode) to emit the light and a photo-diode in the television or equipment to receive the light. A digital code within the controller switches the light on and off, this is then picked up as a digital code at the other end. The communication standard is called 'IrDA' abbreviation for Infrared Digital Association and it allows wireless communication between Mouse, keyboard, joysticks, gamepads etc and receiving equipment such as PC, Laptop, game console.

#### IV. WI-FI

Wifi is maybe one of the most used and successful wireless technologies for data communication. It allows electronic gadgets to exchange data by wireless standard IEEE 802.11. There are many series evolve in IEEE.802.11 standards. The recently introduced version is IEEE 802.11 ac. The Wifi networks are so popular that Wifi facilities are available almost everywhere in daily life; in hotel, campus, home, office, airport, trains, railway station, buses and taxis. In Wifi networks all sort of wireless devices like personal computer, smart phone, video game consoles, TV, wireless sensors etc. It seems that Wifi would play very important role in future generation M2M and heterogeneous networks [12]. The source of Wifi is called access point all the devices in the network can connect to the resource which provides communication facilities such as the local area network and industrial network. The Internet via a wireless network access point come called the hot-spot. Many mobile phone products provide facility to

be a Wifi hot-spot by using cellular networks. The communication range depends upon the used IEEE 802.11 standard, interference, noise, transmitter power and antenna configuration. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves, or as large as many square miles achieved by using multiple overlapping access points [13][14]. For the integrity and security of communication data early encryption standard WEP was introduced which is now replaced with higher quality protocols WPA and WPA2. Wi-Fi Certified 'ac' standardise the latest generation of Wi-Fi which delivers up to gigabit per second data rates, enabling devices to handle demanding applications such as Ultra HD and 4K video, multimedia streaming and rapid file transfer on tablets, gaming devices, handsets and many other devices. This technology would be the backbone of future generation M2M. It is based on IEEE 802.11ac, Wi-Fi certified ac devices offer higher capacity, improved power management, and lower latency to readily handle today's demanding applications while paving the way for new products and services at home, in public places, and in enterprise networks alike. The first Wi-Fi certified product was announced in 2000. The new Wi-Fi standard in Snapdragon will increase peak data transfer rates, but at the same time enable tablets and smartphones to retain battery life similar to mobile devices with 802.11 b/g/n technology. The theoretical data transfer rates for 802.11ac is expected to be three to four times faster than that of 802.11n, which is on mobile devices, PCs and routers today. Wifi provides an alternative to a quality of service via wireless mode as compared to Ethernet Cable Replacement or Mobile office applications, thus reducing the costs for field technical applications. Due to high power requirements, it is not possible in rare cases for communication of sensors/actuator networks. In other words, it is very useful for vertical integration communication in industrial automation.

#### V. CELLULAR MOBILE COMMUNICATION

##### A. GSM 2G

The first major revolution in the digital age of mobile communication was GSM. Which stands for Global System for Mobile Communication is a digital wireless communication developed by European Telecommunication Standards Institute (ETSI). It was developed to replace the analog 1G cellular mobile system and initially described as circuit switch network for full duplex voice telephony. Later it was expanded for voice and data communication. Initially, it was by circuit switched but later it was expanded to packet data communication called GPRS (General Packet Radio Services), GSM, 2G cellular mobile systems. Further, improved data communication rate came in 2.5G cellular mobile system with the use of EGPRS (Enhance General Packet Radio Services), known as EDGE (Enhanced Data Rates for GSM Evolution). GSM technology uses TDMA and FDMA. The GSM was used for voice communication providing bit rates voice service and data transmission service at 9.6 Kbps, 4.8 Kbps and 2.4 Kbps standard named EDGE and GPRS. EDGE is known as 2.5G mobile communication systems. EDGE provides the enhance capacity for data transmission between two devices. In GSM services the network response falls in the range 700ms to

1.5seconds. In worst cases sometimes it falls to 3seconds. The assessment of the working of the device mostly depends upon the polling. For example, if the response time falls to 1.5microseconds then the longer cycles of polling will take place as a result longer configuring of the device. All in all the real time monitoring of the device which is connected wirelessly via 2G seems impossible. For the remote switching via GSM mobile, we can use Siemens 300/1200 PLC series and their respective communication modules.

### B. WCDMA 3G

Later the third generation mobile system developed from 3GPP project by a different consortium and called High-Speed Packet Data Access (HSPDA). HSPDA is known as 3G that was developed to transmit data over the channels. In 3GPP project, a 3G cellular mobile system was developed by Universal Mobile Telecommunication Systems (UMTS) for higher data communication rate, which is not part of GSM standard. In 3G 100ms response time could be achieved. This helps in remote link/communication with the source or device to which it is connected. The 3G networks have higher bandwidth as compared to 2G Networks, which in result help in analysing the real-time monitoring the devices. For example, Cameras could be installed the work location to analyses work in progress at the site and security surveillance etc. Advantages of 3G over 2G are wide bandwidth provision, fast response time and low installation and maintenance cost. Another example of the remote application of 3G is IO Logik W5340-HSDPA could be used for the remote monitoring of the devices in the severe weather conditions where the temperate ranges between -20 –70C.

### C. LTE Advance 4G

Subsequently, 4G cellular mobile system was developed and called as Long Term Evolution Advance (LTE Advance) for higher data communication rate, which also not the part of GSM standard. 4G is a Fourth Generation wireless provide high-speed data rates. It has speed near to the current home broadband network. The download speeds of initial 4G networks is around 5-7 times those for existing 3G networks It is also considered as Ultra Wideband Technology. It provides the high stream data on Laptops/Smartphones and other devices. The major applications are Video Conferencing, VOIP, high-speed gaming content, high definition quality data, high-speed web access and cloud computing. In the context of the Automation 4G technology could be used for the remote monitoring of the plants. Configuration, commissioning and diagnosis can be performed effectively. With the help of 4G, we can obtain high speed comparable to wired internet/Ethernet. This also helps in saving the labour cost and installation of the wired systems with the Desktops. The smart phones can be used for the remote monitoring of the device with the Apps particularly designed for the area to be monitored. As a result of high speed, the multiple locations could be monitored at one with the help of 4G technology [15] [16][17]. In Remote locations, such Windmills solar power plants, water supply systems, RF Antennas this technology can be used as continuous automation and power is not required. It could also be used in tracking of systems with the help of

Global Positioning systems (GPS), for example, monitoring of fleets telemetry.

## VI. REMOTE ACCESS

In this section, the remote access of the automation systems is discussed, which is very important for the modern HMI implementation [19]. Industrial networks are becoming more accessible than ever before from anywhere in the world. Automation engineers are now able to operate the systems and resolve the faults remotely. The engineer able to prepare a plan in advance to fix even the faults couldn't fix remotely. In any case, the remote diagnostic can save a lot of money and time. A corporate network is the set of servers, computers and systems that enables the general functioning of the enterprise IT level. Ethernet TCP/IP is the most common network layer standard used in companies for the development of IT networks at business and enterprise level. Most of the companies linked to the internet via a router and a firewall. Larger corporate networks use additional demilitarized zone (DMZ), which is the part of the networks (mail server, web server, DNS server). Figure 1 shows a schematic overview of how a corporate network is typically linked to the internet. The router in its simplest form is a device that enables communication between two networks. In Figure 1, on the left side, there is a company network (LAN) and on the other hand the Internet (WAN). The Firewalls is used to block unwanted communication. The blocking can be the IP packets filtration according to user-defined rules. Both incoming and outgoing communication can be blocked. The filter criteria can be IP addresses, port numbers or certain protocols which can be either blocked or released.

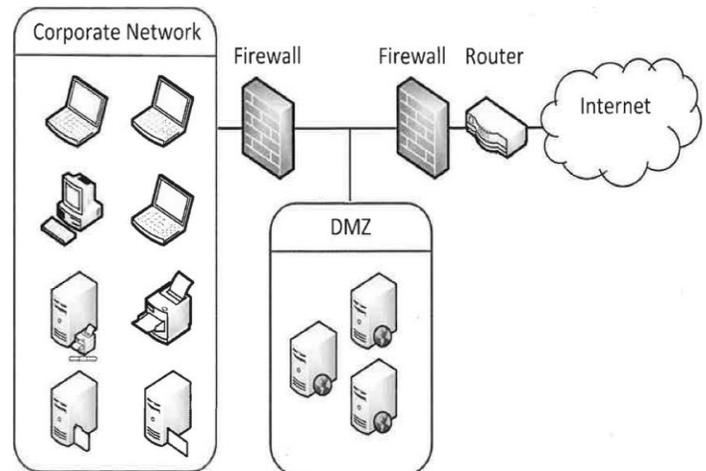


Figure 1: Corporate network

An automation network consists of one or more automation cells. Hereby, each cell is separated by a router, illustrated in Figure 2. In the figure, the automation cell consists of PLCs, data servers, controllers, I/O devices, sensors and actuators that are necessary to carry out various functionalities of the automation system. Switches are the structural elements that

build up the automation cell. The combination of different topologies and media, a flexible, secure and manageable network based on Ethernet TCP/IP can be developed at the field level. In order to create such redundant structures, it is critical that all I/O devices are equipped with an integrated switch. Before pairing the automation network to the corporate network, we usually install a router for the network security. This router ensures an ideal separation between two networks that can have different requirements. This router must be an open and highly secure communication structure between the corporate network and the automation systems. The security ensured by installing a firewall on the link. The firewall is usually installed in the router and mostly configured through browsing to the webpage of the router. The task of the firewall is to block any connections that are not allowed. Remote Access is provided for the people or organisations so that they access a corporate network to use a service on the corporate network or to gain access to a server. In primitive networks, remote access used to obtain by the dial-up connections on the phone.

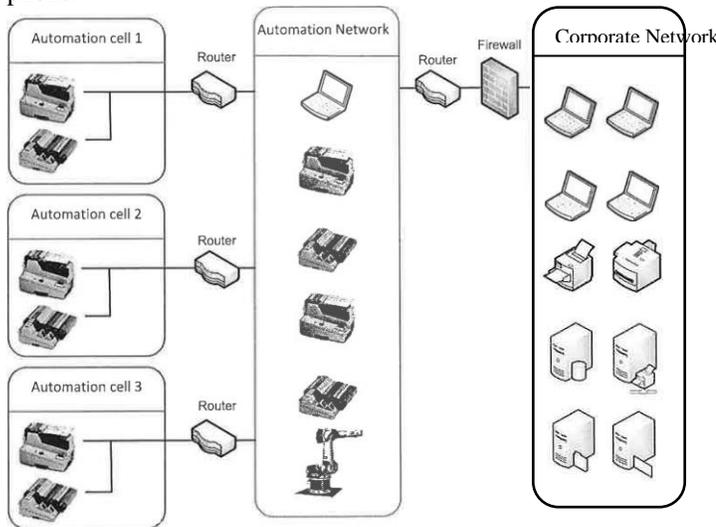


Figure 2: Automation network

Nowadays, remote access can obtain by establishing a virtual private network (VPN) connection. Consider a typical situation in which VPN is used is to link two corporate networks that geographically far apart from each other. In this case, the two networks act as they are one large network, which is important for the operation of some applications.

Automation networks have mostly been isolated networks with controllers and network protocols which are based on proprietary protocols. The production department is usually responsible for industrial communication and they are rarely concerned with security. Modern automation projects are characterised by open systems and communication networks based on Ethernet TCP/IP. This allows the IT department to be partly access and responsible for the industrial communication, which means security is a major concern. Windows and Ethernet are expanding to the production halls and creating

potential network security threats. It has become clear that viruses and hackers are targeting machine parks and installations. Therefore, it is very important to protect automation environments from the dangers that have been common in the IT world for years.

The security of a network is precisely described as follow:

i. layer 1 security

A first step to obtaining a high-secure-network is to secure the network cables, for example, the use of safe clips and seals can prevent network cables from being removed from the network port. Also, the access to free RJ45 ports of the various switches must be complicated mechanically in order to prevent the entry of undesired participants.

ii. Layer 2 security

A second step in securing a network is the use of software for managing switches. Switching should allow the setting of some important protections:

- Web-based management must be secured by a password.
- There should be the ability to assign different privileges based on IP addresses (read-only or read-write protected).
- Switches should offer the facility of setting different devices for each port. For example, a list of allowed MAC addresses can be set per port. Many manufacturers provide industrial switches. One of the examples of the switch is Scalance developed by Siemens.

iii. Endpoint security

Endpoint security means that the end user is responsible for the security of the computer and not to rely only on the firewall or router. This will be necessary when dealing with VPN tunnels because there is a connection between two computers, any of them can be connected to the internet. There should be the careful use of USB sticks. Examples of endpoint security are the use of desktop firewalls, spam filters, and antivirus software. These applications are often integrated into the operating system of the end user. In the case of Microsoft Windows, there is a firewall (Windows firewall) and an antivirus application (security essentials). Also, Internet Explorer should be equipped with all modern safety devices such as phishing filters and anti-spam filters.

VII. EXPERIMENTS

In next subsections, A and B, we have performed two experiments on web panel and operating panel of industrial HMI systems. From these experiments, a comparison analysis is deduced between a web panel and an operation panel and given in Table 1 of the appendix of this paper. An HMI program is developed to complete this set-up. Moreover, an overview is given of different methods to acquire data through the HMI. Two types of HMIs that are often used in industrial environments are operation panels and web panels are demonstrated.

Finally, in subsection C, we have presented an innovative method to control automation systems on various wireless

communication systems. To establish these experiments the following equipment has been used:

- A touch panel of Siemens, KTP400 Basic color PN
- A Siemens S7-1200 PLC, 1212C AC/DCRLY
- A wireless router of Siemens, Scalance W756 series
- A computer, tablet or smartphone for displaying the webpage
- Ethernet CAT6 cables to connect HMI, PLC and router
- Programming software, TIA portal.
- Cellular Mobile Phone Samsung S5
- Laptop Computer Lenovo T420
- Siemens Sinamics S120

A. Implementation of an Operation panel

Figure 3, 4 represents the network with HMI. The operation panel (OP), illustrated in Figure 5. HMI is computer programmed in Siemens software package WinCC flexible. In this first experiment, four input variables and four output variables are programmed and visualised. The variables are representing the inputs and outputs of the PLC. The PLC inputs can be controlled with the dipswitches on the PLC and the status of the inputs signals was monitored on the OP. The PLC outputs are controlled by buttons on the touchscreen of the OP. To enable the communication, a connection between the PLC and the OP needs to be established in the software. Each variable has its properties, which can be adjusted separately. The acquisition cycle time and the acquisition method are shown in Figure 6. There are three acquisition modes: cyclic continuous, cyclic in operation and cyclic on demand. The comparison of the three acquisitions modes is represented in Table 1.



Figure 4 : PLC and HMI in the experimental set-up

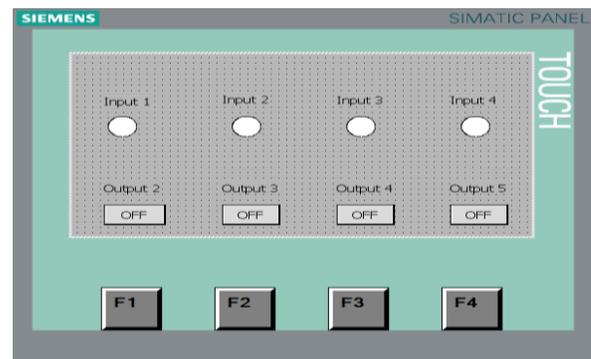


Figure 5: Screenshot of the interface of the OP

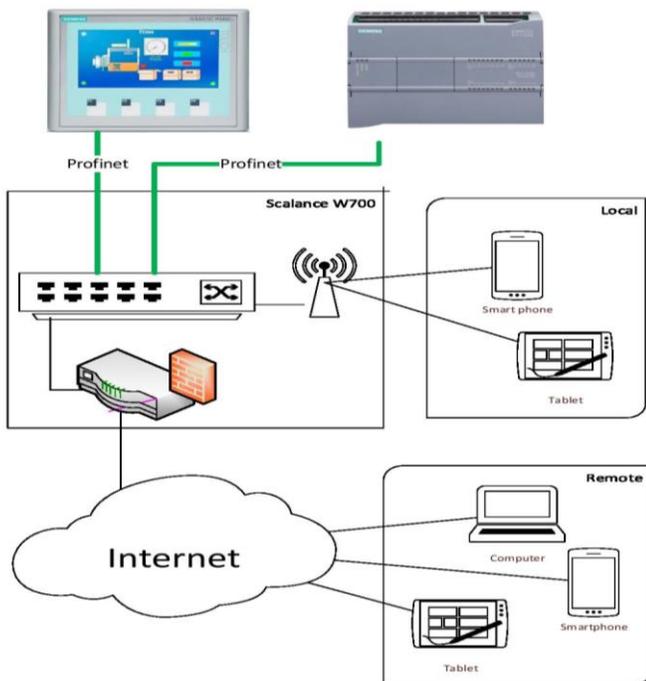


Figure 3: Schematic representation of the experimental set-up

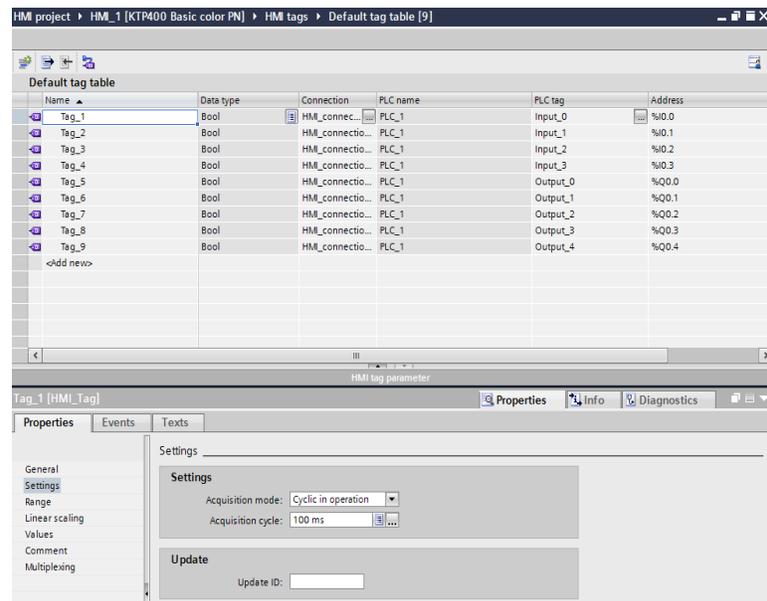


Figure 6: Acquisition cycle time and method for OP variables

Figure 6 shows the properties of a variable of the HMI connection. It is possible to set the acquisition mode of the

different variables separately from each other. For example, when the real-time aspects are the most important, then the cyclic continuous would be set as acquisition mode. In some situations, cyclic continuous can cause an overload on the network, in that case, cyclic in operation acquisition mode is recommended. The third option is on-demand acquisition mode. It is used when a command is given from the user or from an internal request.

In order to make the transmission optimal, variables that are transmitted at the same time will be put in the payload of the same Profinet frame. Only when the payload of one data frame is not sufficient, more than one data frame will be transmitted. This is the fundamental reason why communication between an OP and a PLC is so successful.

#### A. Implementation of a Web panel

In this experiment, the same configuration is used as in the OP, so four input and four output variables are visualised. The variables represent the inputs and outputs of the PLC. The PLC inputs can be controlled by the PLC with dipperswitches. The status of the input signals is monitored on the web panel. The PLC outputs are controlled by buttons on a web page. A user-defined web page, designed in HTML is downloaded to the Siemens PLC. The page displays the state of the machine, such as Alarm, Initialization, and Operation. Also, the page is able to adjust the settings of the machine by means of variables. In order to be able to use the PLC Tags, HTML code needs to be written in the beginning of the HTML file. In this case, the PLC will only update the variables every 10 seconds. Some other PLCs are adjustable to set the update interval to another time. Web panel operation is represented in Figure 7 and Figure 8.

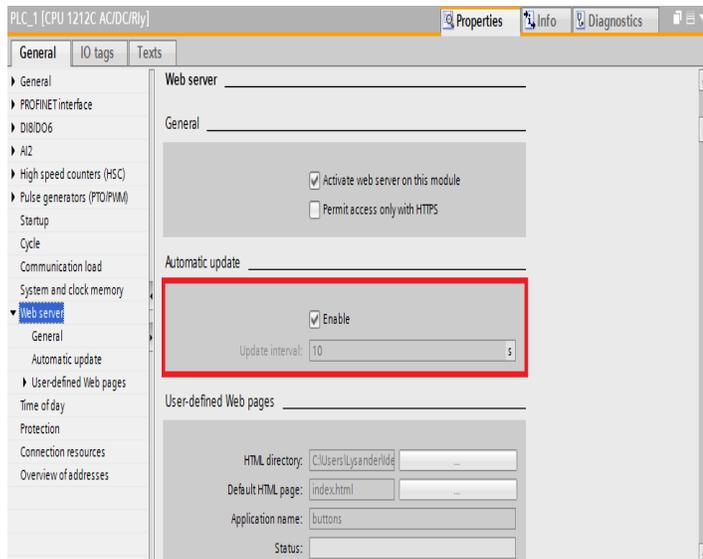


Figure 7: Update interval of the web page

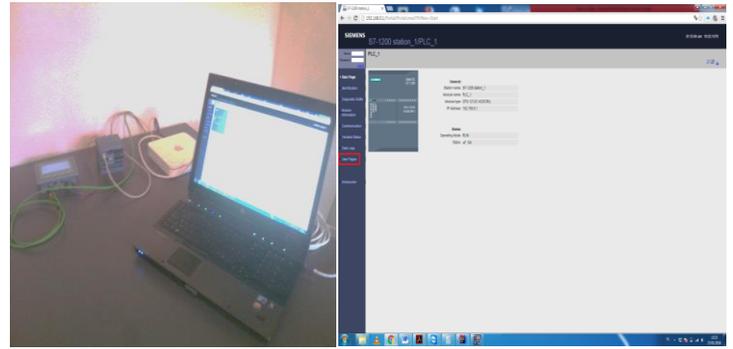


Figure 8: Picture of the set-up with web panel Remote Access

#### C. Innovative Method of Controlling Automation

The set of third experiments are related to the remote control with SCADA/HMI over various wireless standards. In our experiments, we consider the remote control of automation systems by using Cellular mobile phone, laptop computer, smart watch or any portable computer equipment with a display screen. In our experiments, we used Cellular Mobile Phone equipped with the Bluetooth device. For the control purposes, Bluetooth is very suitable to replace serial cables and can be used together with SCADA/HMI to monitor, control and check equipment for maintenance, operation or diagnosis. It has been widely used in industry for the control. The software application used to perform experiments is Victor and Teamviewer. Both these web applications use VPN for the secure connection [3].

These applications can be downloaded to the Mobile Phone and on the remote computer connected with an automation system. A remote connection is established between cellular mobile phone and the remote computer connected to PLC. In our experiment setup, we use Siemens Sinamics S120 Machine and Siemens Programmable Logic Controller (PLC) connected to a Computer. The computer used as programming device and the operational device called PG/PC. It has Siemens Step 7 ver 5.5 software, TIA Portal Version 12 and Siemens Starter software for Sinamics S120. PG/PC and PLC are connected with PROFINET Cable and connection between PLC and Sinamics S120 is PROFIBUS.

Same experimental setup was used for the Infrared, Wifi and Cellular Mobile System. We also used software applications Teamviewer for the remote control of automation systems. We used a Mobile Phone and Laptop connected with the PG/PC and allowed Data Tethering option when we used a mobile phone. The Mobile Phone used as data communication modem. In our experiment, we selected 2G, 3G and 4G options from mobile phone setting and test the control of the systems over these technologies. These communications are shown in Figure 9 and 10. In Figure 9 we performed experiments on the switching Siemens Sinamics and in Figure 10 we have controlled the PLC.

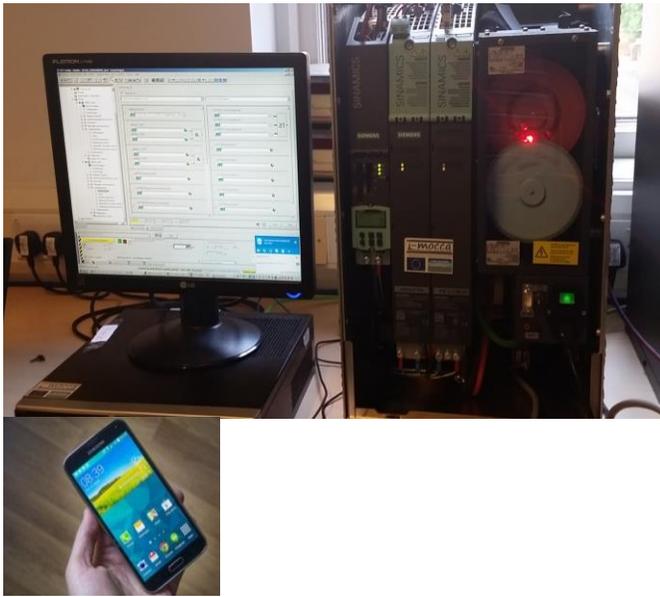


Figure 9:- Automation System Controlled with Mobile Phone by Using Bluetooth, Wifi, 2G, 3G, 4G

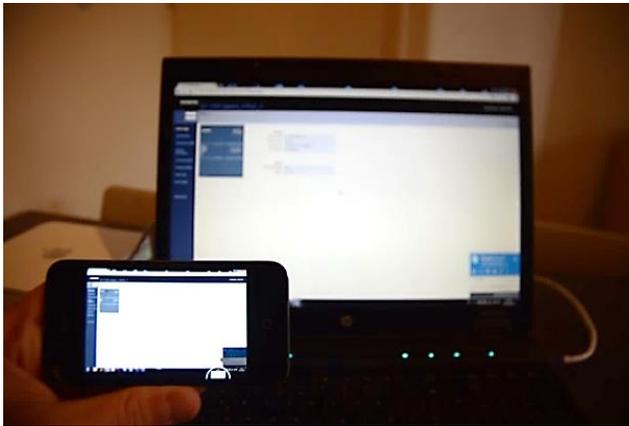


Figure 10: Automation System Controlled by Using, Wifi, 2G, 3G, 4G

### VIII. CONCLUSION AND FUTURE WORK

We have presented the overview of the various wireless technologies, remote control systems and presented various Modern Operating Panels for industrial automation. The Wifi, Cellular, Infrared and Blue tooth mobile networks technologies are very useful in industrial automation systems to control remotely. Various experimental setup of existing HMI systems presented and tested in wireless networks. Finally, an innovative way to remotely control the automation systems by using remote control software application is presented which can efficiently control any automation system remotely on wireless and cellular mobile network. The presented remote control can be easily implemented by various software packages of the remote control.

### ACKNOWLEDGMENT

This research work is generously funded by i-MOCCA, INTERREG-IV Project and University of Greenwich, UK, from October, 2011 to September, 2013. It was presented in the IMOCCA Conference, University of Greenwich, UK.

### REFERENCES

- [1] M. W. Gertz, D. B. Stewart and P. K. Khosla A human machine interface for distributed virtual laboratories vol 1, issue 4, pages 5-13, IEEE Robotics & Automation Magazine, Dec. 1994.
- [2] Friedhelm Nachreiner, Peter Nickel and Inga Meyer, "Human factors in process control systems: The design of human-machine interfaces", Volume 44, Issue 1, Pages 5-26, Safety and Design Elsevier, January 2006.
- [3] Jen-Hao Teng, Kaohsiung, Taiwan, Chin-Yuan Tseng and Yu-Hung Chen, Integration of networked embedded systems into power equipment remote control and monitoring, 566 - 569 vol. 3, TENCON, Nov. 2004
- [4] Besada-Portas, E., Lopez-Orozco, J.A. ; de la Torre, L. and de la Cruz, J.M., "Remote Control Laboratory Using EJS Applets and TwinCAT Programmable Logic Controllers", Vol 56, Issue 2, IEEE Transactions on Education, May 2013.
- [5] Tawfik, M., Sancristobal, E., Martin, S. and Diaz, G., "State-of-the-art remote laboratories for industrial electronics applications", Technologies Applied to Electronics Teaching Conference, 13-15 June 2012.
- [6] Willig, A., Matheus, K. and Wolisz, A., "Wireless Technology in Industrial Networks", Volume:93, Issue: 6, Proceedings of the IEEE, June 2005.
- [7] Andrea Willing, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection", IEEE Transactions on Industrial Informatics, Vol 4 No 2 May 2008.
- [8] Cena G "Wireless Extension of Wired Industrial Communications Networks", 5th IEEE Conference Industrial Informatics, 27 June 2007
- [9] Vitturi, S., Tramarin, F. and Seno, L, "Industrial Wireless Networks: The Significance of Timeliness in Communication Systems", Volume:7, Issue: 2, June 2013.
- [10] Hancke, G.P, Gungor, V.C. ; Hancke, G.P., "Guest Editorial Special Section on Industrial Wireless Sensor Networks", IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, February 2014.
- [11] Jianping Song; Song Han; Mok, A.K.; Deji Chen; Lucas, M.; Nixon, M., "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS08, IEEE, vol., no., pp.377,386, 22-24 April 2008.
- [12] Jaap C. Haartsen, The Bluetooth radio system Personal Communications, IEEE (Volume:7, Issue: 1) 06 August 2002, 28 - 36.
- [13] Jin Shyan Lee, Yu Wei Su and Chang Chou Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee and Wifi", 33 Annual Conference of the IEEE Industrial Electronics, 2007.
- [14] Friedman. R, Kogan. A. and Krivolapov. Y, "On Power and Throughput Tradeoffs of WiFi and Bluetooth in Smartphones", Vol. 12, Issue: 7 IEEE Transactions on Mobile Computing, 17 May 2013.
- [15] Henry, P. and Hui Luo, "WiFi: what's next?" Vol. 40, IEEE, Communications Magazine, 07 May 2003.
- [16] Amitava Ghosh, Rapeepat Ratasuk, Bishwarup Mondal, Nitin Mangalvedhe and Tim Thomas, LTE-advanced: next-generation wireless broadband technology, Pages 10-22, Vol.17, IEEE Wireless Communications Journal, June 2010.
- [17] Lysander Demaiter, "HMI in Industrial Networks", MSc Thesis, Faculty of Engg. & Science, University of Greenwich, UK, March 2016.

## Appendix 1

	<b>Real-time</b>	<b>Deterministic</b>
<b>Operation panel</b>	The data will usually be transmitted in just one or a few data frames, which means that the communication will have a low impact on the network load. Consequently, the delays that occur during transmission are negligible.	As long as only managed routers, such as Scalance are used as network structure elements, Profinet protocols will get a priority. And as long the network is not overloaded, the time of transmitting a Profinet frame can be calculated.
Cyclic continuous acquisition (CCA) mode	The real-time performance of CCA depends on the programme's cycle time. If the processor is too slow to run the programme, the cycle could exceed a certain time, which is therefore not considered as real-time in some applications. With a CPU adjusted to the size of the programme, a cycle time of less than 5ms is realistic. This means the CCA mode gives the best performance on real-time behaviour.	CCA is by definition not deterministic. Depending on the process, the cycle time will vary every time. If requirements are set around deterministic behaviour, CCA mode is not applicable.
Cyclic in operation acquisition (COA) mode	Regardless of the time the processor needs to run the programme, the acquisition of the variable will be completed within fixed cycle time. The cycle time can be adjusted according to the system requirements.	Given that the acquisition cycle time is predefined, COA mode is perfectly deterministic.
On demand acquisition (ODA) mode	The trigger to acquire data could either come from the user or even from the application, i.e. when an analog signal exceeds a certain value. ODA mode will not present the value of a given moment, which means it is not real-time.	As the trigger of acquisition is known, ODA mode is perfectly deterministic.
<b>Web panel</b>	As not only the variables, but also the layout, needs to be transmitted over the network, numerous data frames are required. Therefore, this kind of communication will have a considerable impact on the network load. However, as long as the network capacity is adapted to it, a real-time behaviour is possible.	In order to transmit the HTML web page, TCP/IP is used. And since TCP/IP is using CSCA, it is impossible to calculate the transmission time, meaning, it is not possible to obtain a deterministic result.

Table 1: Comparison of Web Panel and Operating Panel