iJET EXPLORE International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 3 No. 12, December, 2013

Wireless Sensor Networks for SCADA and Industrial Control Systems

Action Nechibvute, Courage Mudzingwa
Department of Applied Physics and Telecommunications, Midlands State University, Private Bag 9055 Gweru, Zimbabwe

ABSTRACT

In traditional supervisory control and data acquisition (SCADA) systems, most sensors are wired, which limits their use. Integrating Wireless sensor networks (WSNs) with SCADA and industrial control systems would make monitoring more flexible. Integrated SCADA and WSN capabilities raise the possibility of realising flexible, maintenance-free systems suitable for most industrial and field operations using low power, battery-operated solutions that offer a low cost, wireless alternative to traditional cabled systems. In this work, we discuss the potential benefits and challenges that are encountered when WSNs are integrated into process automation systems.

Keywords: *wireless sensor, networks, SCADA, industrial control, automation*

1. INTRODUCTION

The application of Wireless Sensor Networks (WSNs) in industry is gradually being adopted particularly for process monitoring, control and data processing [1-5]. WSN technology brings several advantages over traditional wired industrial monitoring and control systems, including self-organization, rapid deployment, flexibility, and inherent intelligent processing [4]. WSN based automation systems will greatly offer new and more effective functions and solutions which traditionally could not be met through the conventional wired instrumentation systems [3-8].

WSNs are formed from a collection of miniature autonomous devices with sensors embedded in them, called sensor node [6,7]. A typical node include the following basic components: power unit, sensor unit, processing unit, memory unit and communication unit (See Figure 1). The power unit is usually a battery, which acts as the power source for all the components of the sensor nodes. It is important that the sensor network should be able to perform the monitoring operations of the environment for a sufficient time (which could be days or months). The battery lifetime may not be compatible with the expected performances of the node; it is therefore required to scavenge energy from the external environment [8-10]. The sensor unit consists of a group of micro-electromechanical system (MEMS) - based sensors (and actuators) used for data acquisition from the physical environment. The processing unit which includes a microprocessor or a micro-controller is responsible for management of data acquisition, handling communication protocols, scheduling and preparation of data packets for transmission once it has gathered, filtered, and synchronised the data from the sensors [10-13]. The communication unit consists of a short range RF transceiver for wireless communication. The individual nodes are capable of sensing their environments, processing the information locally, or sending it to one or more collection points through a wireless link [11,12]. WSNs present a novel technology, which has advantages of distributed information processing, broad coverage, and remote monitoring and control [6,7,12].

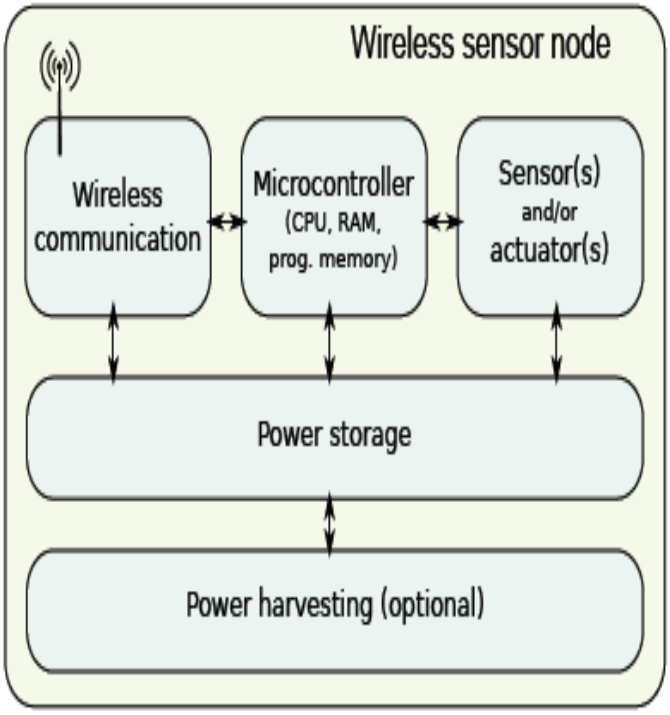

Figure 1: Typical hardware components of a wireless sensor node

Traditionally, Supervisory Control and Data Acquisition (SCADA) systems have been widely used in automation and industrial production where a plethora of different wired sensor systems is employed [13-15]. Most of these sensors are wired to a machine or factory floor network; while some of them are already connected wirelessly. WSNs have the potential to be the integral part of the next generation industrial control and automation systems since they have the potential of significantly

improving the sensing capabilities of SCADA sub-systems, as well as of increasing the resilience of the overall SCADA architecture.

In this paper we discuss the adoption of WSNs as an integral part of the next generation SCADA and industrial control systems. The paper is organized as follows: Section 2 provides an overview of SCADA and SCADA systems. Section 3 discusses the industrial WSNs, Section 4 overviews the industrial WSNs for SCADA and process automation. Section 5 discusses the challenges and potential solutions that need to be addressed for successful integration and applicability of wireless instrumentation. Finally, the paper is concluded in Section 6.

2. OVERVIEW OF SCADA SYSTEMS

2.1 Components of SCADA Systems

SCADA is a technology that enables the user to collect data from one or more distant facilities and/or send limited control instructions to those facilities [13]. It can be alternatively described as a system operating with coded signals over communication channels so as to provide control of RTU (Remote Terminal Unit) equipment [13-15]. Traditionally, the majority of SCADA systems are designed for more closed and controlled industrial environments. However, there has been an integration of enterprise systems and large scale services to enhance their functionality while minimizing overall operation cost.

A typical SCADA System consists of several subsystems notably [14-17]:

1. Field data interface devices: Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs) which collect data from the field deployed sensors make the necessary adjustments and transmit the data to the monitoring and control system. PLCs are frequently used as alternatives to RTUs since they are more economical, versatile, flexible, and configurable than special-purpose RTUs [18].

2. The communication infrastructure used to transfer data between field data interface devices and control units and the computers in the SCADA central host. The infrastructure can be radio, telephones, cables, satellites, or any combination of these.

3. A central host computer server or servers (sometimes called a SCADA Centre, Master Station, or Master Terminal Unit (MTU). The computer does the monitoring (gathering of data) as well as the control (actuation) of the linked processes.

4. A collection of standard and/or custom software sometimes called Human Machine Interface (HMI) software or Man Machine Interface (MMI) software systems used to provide the SCADA central host and operator terminal application, support the communications system, and monitor and control remotely located field data interface devices.

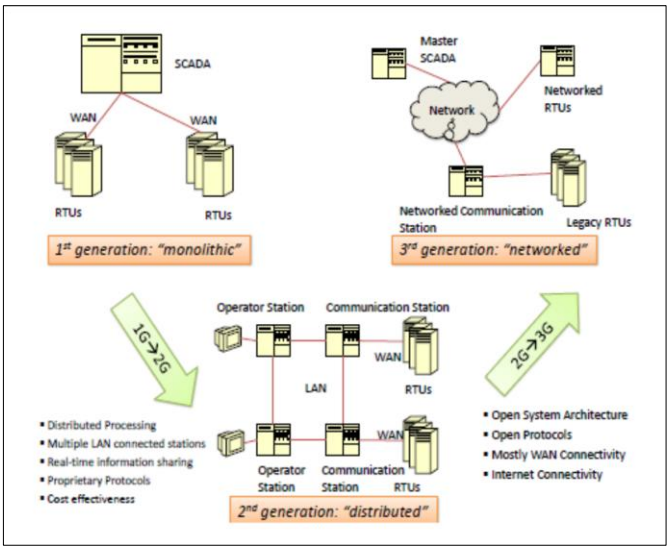

Figure 2: Evolution of SCADA systems [18]

When SCADA systems were first developed, the concept of computing in general centred on "mainframe" systems [17]. Networks were generally non-existent and each centralized system stood alone. As a result, first generation SCADA systems were standalone and monolithic with virtually no connectivity to other systems. The Wide Area Networks (WANs) that were implemented to communicate with remote terminal units (RTUs) were designed with a single purpose in mind: –that of communicating with RTUs in the field and nothing else. However, the next generation of SCADA systems took advantage of developments and improvements in system miniaturization and Local Area Networking (LAN) technology to move towards a more distributed flavour where LAN was used to interconnect the components (see Figure 2). This approach was more cost effective than the first generation and allowed distributed processing and real-time information sharing among the entities based on proprietary protocols [17,18]. As was the case with the first generation systems, the second generation SCADA systems were also limited to hardware, software, and peripheral devices that were provided or at least selected by the vendor. The emergence of the third generation moved towards utilizing the network as such, using not only WAN but also Internet, and featured open system architecture and open protocols [15,18]. The distributed processing across physically separate locations has enabled the design of SCADA systems that can survive a total loss of any one location. For some organizations that see SCADA as a super-critical function, this is a real benefit. The next generation will push further the limits in the network, adopting WSNs to enhance the capabilities of SCADA systems [5,18].

2.2 Challenges to conventional SCADAs

While SCADAs are the mainstay of most automation systems in industry, they have their own challenges. As noted by Ye [20],

the major challenge of conventional SCADA systems is their inflexibility, static and centralized architecture which significantly limits their interoperability with other networks technology or systems. Generally SCADA systems are expensive to deploy and maintain. This is particularly so for applications such as pipeline network in oil and gas fields [19]. Proprietary SCADA systems tie their customers to one specific control device manufacturer, creating a difficult negotiating position for customers during future purchases [20]. Legacy SCADA systems which still dominate the automation and telemetry implementations lack compatibility with other systems and thus limit scalability. SCADA has low data and low data update rates making it inefficient in such systems as Smart Grid Applications [21-23].

2.3 Potential benefits of WSNs in SCADA and Automation

Reduced Maintenance and Deployment Costs: Wireless sensor nodes eliminate cabling and trenching cost of deployment by up to 70 % [24]. Unlike its wired counterpart, wireless devices can be deployed in areas that are both physically inaccessible and cost prohibitive for example - monitoring and control devices for rotary equipment [25]. WSNs offer easy maintenance since problems like corrosion, water in the conduit, burned cabling, freezing, wild animal damage, ,and physical wear caused by frequent encounter in wired systems are eliminated.

High levels of Scalability and Flexibility: Wireless devices can be easily relocated and reorganized without tedious work of removing old cables and laying out new ones [24,25] Furthermore, the industrial process system becomes highly scalable and flexible due to the device autonomy [25-28]. Wireless systems are battery powered, newly added devices can be installed at any location without running power supply and data communication wires through concrete walls during factory expansion. On the contrary, wired systems can take days or weeks to install, whereas wireless instruments require only the sensor to be installed in the process, saving time and valuable resources. The rigid design of current RTUs reduces the flexibility of SCADA systems [19,20].

Improved Resource management in a control system: WSN enabled systems make real-time decisions based on measurements taken while an industrial process is running. Measurement data from the wireless sensors can be readily utilized for both dynamic control of industrial process and display over a network to allow remote monitoring of the process status in real-time. Abnormal conditions (e.g. rising or falling pressures, temperatures, or vibrations) may be easily flagged up as fault conditions. As data is collected as part of a SCADA system, it can also be archived for future reference [29-31].

Improved Performance: WSN enabled automation systems have the potential to outperform the existing wired process control systems. Firstly, industrial WSNs allow higher data transmission speed. For example, the most popular control protocols HART (Highway Addressable Remote Transducer) has a data rate of 1.2 kbps and FF (Foundation Fieldbus) has a data rate of 31.25 kbps, while WirelessHart has a data rate of 250 kbps based on the IEEE 802.15.4 standard. Secondly, unlike wired control systems, where devices share a single bus, multiple wireless communications can act simultaneously if there is no mutual radio interference [25,30] .Thirdly, more sensors/data points can be used to beat the performance of traditional wired control system

.

Exploitation of Micro-Electromechanical Systems (MEMS): MEMS devices integrated with computational power and communication capabilities offer a more robust design than attaching wires to small-sized devices [32].This means embedded sensor systems can be applied widely, including in production lines, (See Figure 3).

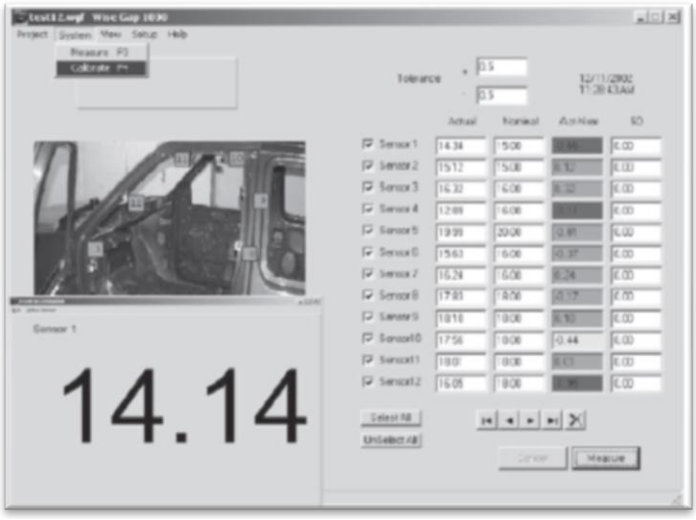

Figure 3 Application of WSNs in production line [33]

Table 1: comparison between SCADA and WSN[19]

Characteristic	SCADA	WSN
Architecture	Centralized	Decentralized
Storage & Control	Central site	Local Sensor node
Flexibility	Inflexible	Versatile
Cost	Expensive	Low
Node Density	Low	High
Data Rate	Low	High
Network Protocol	Proprietary	Non-proprietary

3. INDUSTRIAL WSN REQUIREMENTS

3.1 Application Specific Requirements

There are strict regulations that govern the installation of wires in some industrial environments, particularly in the oil and gas sector. As a result of the strict regulations associated with the installation of wired sensors on oil and gas platforms, the introduction of WSN devices is complicated, time-consuming

and expensive. WSNs deployments in such environments and manufacturing industries need to be highly reliable and compatible with the existing wired systems. The performance of these sensors often determines the success of the manufacturing operation itself. If the sensors do not perform their mission large amounts of valuable production or production time may be lost. Wireless sensors need to be designed specifically to fulfil an industrial mission [33]. The ISA SP100 workgroup classified the industrial processes into three broad categories and six classes of WSN usage (from Class 0 to Class 5) as shown in Table 2 [34]. Table 3 shows some of the network requirements in industrial process automation.

The design of networked control systems has to take into account a large number of factors that ensure correct implementation and different industrial applications will have very different needs and will choose different solutions, values, or bounds for each of these variables. The real objectives for any wireless industrial product are determined by the manufacturing operation in which it must perform, not by the technology employed. Some of the most critical requirements are system performance in terms of data transmission rate and sample rate, communication reliability and power supply. The last one is especially critical in the context of WSNs, because the network must be able to operate for long periods without the need of system service, which would require human involvement. In addition to automatic network initialization, self-diagnostic and self-healing operations, it is also important to be able to perform intelligent operations in the network in a distributed manner.

Table 2: Application needs of industrial process by usage [34]

Safety	Class 0: Emergency action (always critical)
Control	Class 1: Closed loop regulatory control (often critical)
	Class 2: Closed loop supervisory control (usually non-critical)
	Class 3: Open loop control (human in the loop)
Monitoring	Class 4: Alerting; Short-term operational consequence (e.g event based maintenance)
	Class 5: Logging & downloading/uploading No immediate operational consequence (e.g. history collection, preventative maintenance)

Table 3: Typical requirements for industrial wireless sensor and actuator networks in the process automation domain [35]

Sensor Network Applications	*Delay*	*Range*	*Battery Lifetime*	*Update Frequency*	*Security Level*
Monitoring and supervision					
Vibration sensor	S	100 m	3 years	Sec-days	Low
Pressure sensor	Ms	100 m	3 years	1 sec	Low
Temperature sensor	s	100 m	3 years	5 sec	Low
Gas detection sensor	ms	100 m	3 years	1sec	low
Closed loop control					
Control valve	ms	100 m	5 years	10-500ms	Medium
Pressure sensor	ms	100 m	5 years	10-500ms	Medium
Temperature sensor	ms	100 m	5 years	500ms	Medium
Flow sensor	ms	100 m	5 years	10-500ms	Medium
Torque sensor	ms	100 m	5 years	10-500ms	Medium
Variable speed drive	ms	100 m	5 years	10-500ms	Medium
Interlocking and Control					
Proximity sensor	ms	100 m	5 years	10-250ms	Medium
Motor	ms	100 m	5 years	10-250ms	Medium
Valve	ms	100 m	5 years	10-250ms	Medium
Protection relays	ms	100 m	5 years	10-250ms	Medium

3.2 Performance Issues

In this section we discuss some major issues that need to be addressed in order to achieve a large scale deployment of WSNs in industrial automation

Reliability: It is the measure of the percentage of accurate data which reaches its destination. The ability of the network to ensure reliable data transmission in a state of continuous change of network structure [35-37]. Packet loss in wireless sensor networks is usually due to the quality of the wireless channel, sensor failure, and congestion. Most of the applications need reliable transmission of each packet, and thus packet-level reliability is required. Wireless instrumentation must be as reliable as conventional wired units. Radio interference is certain, and the sensor network must be able to perform its mission in the presence of many types of radio interference.

Scalability: It is the ability of the network to grow, in terms of the number of nodes, without excessive overhead- represents

the maximum number of generated key rings which corresponds to the maximum number of supported nodes [38]. A large scale secure deployment of sensor networks relies strongly on this performance metric [38-41]. The number of sensors in a single production unit can vary from a few to several thousands.

Adaptability: It is a measure of time delay. It is defined as the time it takes from when a data packet is transmitted from the originating sensor to reach its final destination [42].
Latency: **T**he time required for a sensor reading to reach the automation system must be bounded if the sensor data is used in a closed-loop control system. The upper limit of this bound depends upon the application. It can range from seconds to just a few milliseconds [43,44]

Control loop cycle times: Process automation control loop cycle times are normally in the range of seconds to minutes, while machine control loop cycle times are normally in the range of milliseconds [45,46].

Range: The sensor network will need to communicate reliably over a specified distance. Some production equipment is compact, and some is very large. Multiple wireless hopping is typically employed since the inter-sensor communication is within short transmission ranges due to energy and bandwidth limitations [47].

Power Efficiency: This is the ability of the network to operate at extremely low power levels. The sensor will need reliable battery power (with its disadvantage of additional service intervals) or some other source of energy. The lack of battery replacement, which is essential for affordable WSN deployment, requires energy-efficient operations. Since high reliability and low delay may require significant energy consumption, the reliability and delay must be flexible design parameters that still meet the requirements [48,49].

Data Types: There are both analog and discrete output sensors, and in addition some "smart" sensors may supply diagnostic information that can also be used to improve the reliability or quality of production.

Sensor Traffic Patterns: The type and amount of data to be transmitted is also important when considering control applications [47-49]. Control signals can be divided into two categories: real-time and event based. For real-time control, signals must be received within a specified deadline for correct operation of the system. In order to support real-time control, networks must be able to guarantee the delay of a signal within a specified time deadline. Hence, heavy traffic may be generated if sensors send data very frequently. Event-based control signals are used by the controller to make decisions but do not have a time deadline [50]. The decision is taken if the system receives a signal or a timeout is reached.

4. INDUSTRIAL WSNs FOR SCADA & PROCESS AUTOMATION

4.1 WSN Interfacing Automation Systems

WSNs are principally an enabling technology that can further push the limits of the current networked SCADA systems. Firstly, the WSNs can be potentially used as a replacement for the remote terminal units (RTUs) in conventional SCADA systems. In the context of wireless automation, WSN usually operates as a part of the automation system and hence issues of interfacing and compatibility with other parts of the system are critical. It must be noted that the WSNs for SCADA systems are unique; and are different from the generic WSNs. The key differences to be noted are [51]:

- There is an online trusted third party (monitoring station).
- There is no aggregation: the controller collects all the data coming in from the sensors.
- The battery life of the sensors is expected to last several years; therefore, the energy efficiency of the protocols is not as critical as in other applications of sensor networks.
- Although there are some implementations of multi-hop routing, the majority of current deployments use a single hop between the sensors and the gateway.
- Sensors must be accessible and configurable by handheld devices used by network operators.

WSNs can be interfaced to SCADA systems and other wired automation control platforms by means of specially designed middleware. The middleware frameworks can be used to capture the data from the WSNs and distribute pre-sorted and translated information to the SCADA system. A practical example is SensiLink™ which is a middleware and software suite from MeshNetics that links WSNs with SCADA systems [52,54]. Sensor data collected from the nodes is channeled through RS232, RS485, USB, Ethernet, or GPRS gateway to the SensiLink server. ArchRock [55], Octavex [56], and SnapSense OneClick [57] are some of the middleware that can be used in the integration of WSNs to the process automation platforms. Alternative approaches can also be realised by means of Peer to peer (P2P) protocols (for example HourGlass [58], and P2PBridge[59,60],]) and the use of sensor network gateways functioning as bridges [61,62]

4.2. Industrial WSNs for Process Automation

ZigBee [63], WirelessHART [64] and ISAI00.11a [65] are the most popular standards for industrial wireless devices and networks [66]. Unlike the ZigBee standards which are insufficient to fulfil the strong reliability requirements of

process automation, the WirelessHART and ISA100.11a standards offer the most complete set of mechanisms with channel blacklisting and frequency hopping to avoid perturbations caused by interference. Major international automation and control companies have developed applications of wireless instrumentation technologies based on the Wireless HART and/or ISA100.11a. The companies of note in this field are Honeywell [67], Emerson [68], ABB [69], Rockwell [70] and Yokogawa[71]. This section discusses the fundamentals of WirelessHART and ISA100.11a networks

(a) WirelessHART network: System overview

The following devices and components are associated with a WirelessHART network [64]:

1. Field Device: A field instrument with integrated wireless communication.
2. Adapter: A wireless communication module that connects to wired HART field devices, providing them with WirelessHART capabilities.
3. Handheld: A portable WirelessHART computer used for configuration, diagnostics, and calibration of field devices.
4. Gateway: A network access point that connects the WirelessHART network to a plant automation network, allowing the data to flow between the two.
5. Network Manager: An application that manages the WirelessHART network and its devices.
6. Security Manager: An application that is responsible for generating, storing, and managing join, network, and session keys.

(b) ISA 100.11a: System overview

An ISA100.11a device shall hold one or more of the following roles [65]

1. Input/Output (I/O): A device that provides data (sensor) to or uses data (actuator) from other devices.
2. Router: A device that is capable of routing data from other devices in the network.
3. Provisioning: A device that is capable of provisioning other devices, enabling them to join a specific network.
4. Backbone Router: A device that is capable of routing data to/from a backbone network.
5. Gateway: A device that provides an interface between the wireless and the plant network or directly to an end application on a plant network.
6. System Manager: An application that governs the network, network devices, and network communications.
7. Security Manager: An application that, in conjunction with the system manager, provides a secure system operation.
8. System Time Source: A device that is responsible for maintaining the master time source for the system.

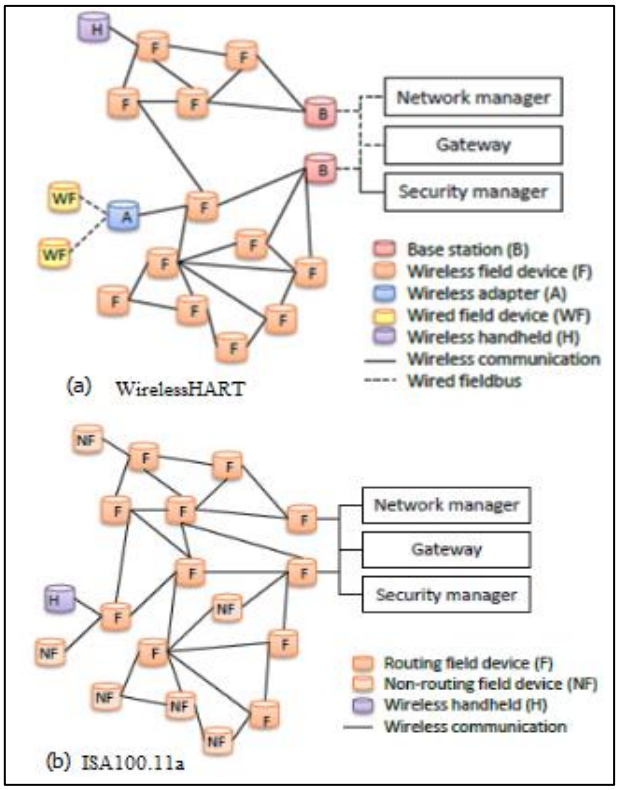

Figure 4 Network Elements: WirelessHART and ISA100.11a [64,65]

The reader is referred to [72] for details of the competing features of WirelessHART and ISA100.11a standards. Table 4 gives a review of the standards.

Table 4: Table 5 ZigBee, WirelessHART, and ISA100 Characteristics [38,63-65,72]

Protocol layers	ZigBee	WirelessHART	ISA100.11a
PHY layer	IEEE 802.15.4-2003 with 868 MHz/915 MHz or 2.4 MHz radio	IEEE 802.15.4-2006 with 2.4 MHz radio only	IEEE 802.15.4-2006 with 2.4 MHz radio only
MAC layer	IEEE 802.15.4-2003 with a low frequency hopping schema. No deterministic access methods	IEEE 802.15.4-2006 with TDMA + Channel hopping or Token-passing method	IEEE 802.15.4-2006 with an extension shim for frequency hopping and slotted hoping No deterministic access methods

Network Topology	Star, Mesh	Tree, Star, Mesh	Star, Mesh
Network Scalability	16-bit node address and 16-bit group address or 64-bit extended network address	16-bit network address,16-bit nickname and 64-bit address	64-network address and 64-bit device address
Network routing Strategy	Mixed mechanism composed of AODV and tree routing No energy aware routing strategy	Graph routing (link state routing) No energy aware routing strategy	Graph routing (link state routing) No energy aware routing strategy
Description	A mesh-networking standard for control and monitoring; building/home automation, embedded sensing. Range of up to 50m	A multi-vendor standard specifically designed for process monitoring and control; mesh networking with large numbers of sensors/nodes. Range is less than 100 feet	A multivendor standard for reliable and secure wireless connectivity for Non-critical control and monitoring. Low data rate, very low power consumption. Range of 600m
Advantages	Low-cost, power efficient, easy solution for small networks. Use is wide spread	Designated as an international standard. Built on a 30-year old HART technology. An accepted standard. Specifically created for industrial controls	Can scale above 250 nodes per network. An accepted standard. Crated specifically for industrial controls
Disadvantages	Cannot serve a high number of nodes within the specified period	Not compatible with some existing wired protocols (FieldBus,Profibus,)Up to 250 nodes on a network	Not yet in wide use. Communicates with HART, Fieldbus Modbus,Profibus

5. CHALLENGES AND POTENTIAL SOLUTIONS

1) Harsh Industrial conditions

The harsh industrial conditions present a challenging operating environment for WSNs and the associated wireless device. The WSN are expected to work reliably over a range of operating temperatures, and to sustain strong vibrations, excessive electromagnetic noise caused by large electromechanical equipment [73]. In addition to this noisy environment, the WSNs should withstand the atmospheric precipitation, condensation and airborne contaminants present [74, 75]. Furthermore, the signal might be subject to heavy multipath propagation effects caused by multiple reflections from mainly metallic structures in the surrounding environment. The random/periodic movement of workers, industrial robots, trucks, and other objects may also cause time varying channel conditions. These propagation impairments to mission-critical signals in industrial settings can result in costly disasters in terms of money, manpower, time, and even human lives [76,77]. The Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS) technology has been utilized to significantly reduce noise interference Redundant technique-dual gateways are highly recommended for increased reliability [25]. However more research efforts on designing the WSN for industrial environments is needed. A typical research approach is investing in WSN testbeds (for example WINTeR [78]) that mimic the industrial surroundings with complex multipath propagation shemes. Better still would be intensive study using testbeds such as GINSENG [79].

2) Data and Network Security

Sensor nodes are not tamper resistant due to cost constraints; any human user or machine can reprogram them or simply destroy them. Passive attacks on WSNs are able to retrieve data from the network, but do not influence over its behaviour. On the other hand, active attacks directly hinder the provisioning of services [80]. These security attacks directly affect the energy consumption and due to the large amount of energy consumed at the MAC layer, it
is particularly vulnerable to many different security attacks. More research on behavioural modelling of security attacks is needed [81]. Currently, the wired fieldbuses connecting

SCADA and automation system to WSN devices lack security extensions. This loophole is potentially a severe challenge since scalable and modular solutions cannot be provided when integrating new wired/wireless devices into existing automation systems [82]. To secure IP-based SCADA systems, it is vital to implement secure architectures which prevent access to the SCADA from corporate IT and other third-party networks and to enforce excellent management practices to manage IP-based networks [83]. As noted by Cardenas et al [84], there are many research challenges that need to be addressed particularly the development of systematic analysis of the threat model and its relation to the security countermeasures, the precise definitions of security metrics, and the detailed study of real world deployment scenarios.

3) Quality of Service (QoS) Issues and resource constraints

The deployment strategies of WSN in industrial automation systems for coverage and connectivity enhancement are critical to the (QoS) of the networks. The guarantee of QoS typically considers multiple factors, for example,
electromagnetic interferences, accidental death of sensor node, dynamic network topology, low
processing capability, and small memory capacity [85]. Furthermore, the design and implementation of WSNs is constrained by three types of resources: a) energy; b) memory; and c) processing [7,11,51];- which makes it hard to maintain the QoS [86]. Current research output on energy harvesting and novel energy management will potentially contribute significantly in addressing the energy constraints in WSNs. However, due to refresh rates required in process automation it is difficult to save much energy by minimizing the duty cycle of a wireless field device [87].

6. CONCLUSIONS

In this article, a discussion of the main issues involved in the application of WSNs in SCADA and industrial control systems. There is need for efficient integration of the WSNs into existing automation to achieve a seamless transition from wired to wireless communication, as well as simple deployment, commissioning, and maintenance. Despite outstanding research issues on security, reliability and QoS, WSN-enable automation systems will get more popular, largely due to the greatly increased flexibility, lower cost and scalability that could not be obtained from the traditional all-wired automation systems.

REFERENCES

[1]. V.C. Gungor, G.P. Hancke, (ed), "Industrial Wireless Sensor Networks: Applications, Protocols, and Standards,",CRC Press, 2013.

[2]. D. Christin, P. S. Mogre, and M. Hollick, "Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives," *Etude de la notion de pile applic l'analyse syntaxique*., pp. 96–125, 2010.

[3]. A. Ray, J. Akerberg, M. Gidlund and M. Bjorkmany, "Initial Key Distribution for Industrial Wireless Sensor Networks," *IEEE Int. Conf. on Ind. Tech. (ICIT 2013)*, Cape Town, South Africa, 2013.

[4]. V.C. Gungor and G.P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles and Technical Approaches", *IEEE Trans. on Ind. Elect*., vol. 56, no. 10, pp. 4258 – 4265, 2009.

[5]. C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," *IEEE Trans. on Systems, Man, and Cybernetics*, vol. 40, no. 4, pp. 419 –428, 2010.

[6]. D. Culler, D. Estrin, and M. Srivastava, "Overview of sensor networks," *IEEE Computer*, pp. 41–49, Aug. 2004.

[7]. I. F. Akyildiz, T. Melodia, and K. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Netw*., vol. 51, no. 4, pp. 921–960,Mar. 2007.

[8]. J. M. Gilbert and F. Balouchi, "Comparison of Energy Harvesting Systems for Wireless Sensor Networks," *Int. J. of Autom. and Comp*., vol. 5, no. 4, pp. 334-347, 2008.

[9]. A. Nechibvute, A. Chawanda and P. Luhanga, "Piezoelectric Energy Harvesting Devices: An Alternative Energy Source for Wireless Sensors," *Smart Materials Research*, Article ID 853481, 2012

[10]. Y-J Yoon, W-T Park, K. Li, Y. Ng, Y. Song; *Int. J. of Precision Eng. and Manuf*., vol. 14, no.7, pp. 1257-1262, 2013.

[11]. I. F. Akyildiz and M. C. Vuran, "Wireless Sensor Networks," *Wiley*, 2010

[12]. W. Dargie and C. Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice," *Wiley*, 2010

[13]. D.J Gaushell, "Supervisory control and data acquisition," *Proc. of the IEEE*, vol. 75, no. 12, pp. 1645 – 1658, 1987.

[14]. G. Carke, D. Rynders, E. Wright, "Practical Modern SCADA Protocols," *Elsevier*, 2003.

[15]. Technical Information Bulletin 04-1, Supervisory Control and Data Acquisition (SCADA) Systems, *NCS TIB04-1*, Oct. 2004

[16]. D.Bailey and E. Wright, "Practical SCADA for Industry," *IDC Technologies*, 2003

[17]. R. L. Krutz, "Securing SCADA Systems," *Wiley*, Indianapolis, 2006.

[18]. S. Karnouskos, A. W. Colombo, "Architecting the Next Generation of Service-based SCADA/DCS System of Systems", *in Proc. 37th Annual Conference of the IEEE Ind. Elect. Society (IECON 2011)*, Melbourne, Australia, pp. 359-364, 2011.

[19]. S. Yoon, W. Ye, J. Heidemann, B. Littlefield, and C. Shahabi, "SWATS: Wireless Sensor Networks for Steamflood and Waterflood Pipeline Monitoring," *CiSoft*, 2008.

[20]. W. Ye and J. Heidemann, "Enabling Interoperability and Extensibility of Future SCADA Systems," Technical Report USC Information Science Institute 2006.

[21]. V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. on Ind. Elect.*, vol. 57, no. 10, pp. 3557–3564, 2010.

[22]. V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Comp. Netw*., vol. 50, no. 7, pp. 877–897, 2006.

[23]. Y. Liu, "Wireless Sensor Network Applications in Smart Grid: Recent Trends and Challenge," *Int. J. of Dist. Sensor Netw.*; vol. 2012, Article ID 492819, 8 pages

[24]. H. Fouda, "Improving SCADA Operations Using Wireless Instrumentation," Control Microsystems" White Paper, www.controlmicrosystems.com

[25]. G. Zhao, "Wireless Sensor Networks for Industrial Proces Monitoring and Control: A Survey," *Network Protocols and Algorithms*, vol. 3, vo. 1, pp.46-63, 2011.

[26]. M. Antoniou, M. C. Boon, P. N. Green, P. R. Green and T. A. York, "Wireless sensor networks for industrial processes," *IEEE Sensors Applications Symposium*, pp.13-18, 2009.

[27]. M. Hanssmann, S. Rhee, and S. Liu, "No wiring constraints," *IEEE Ind. App. Mag.*, pp. 60-65, 2009

[28]. S. Yoo, P.K. Chong, D. Kim, Y. Doh, M.-L. Pham, E. Choi, and J. Huh, "Guaranteeing Real-Time Services for Industrial Wireless Sensor Networks With IEEE 802.15.4. *IEEE Trans. Industr. Electron.* , vol. *57*, pp. 3868–3876, 2010.

[29]. Wireless sensors enjoy timely role in factory automation; Industrial Ethernet Book Issue 57 / 35; http://www.iebmedia.com

[30]. P. Vyas, "Wireless Sensor Networks for Industrial Process Monitoring and Control with Security Architecture: A survey for Research Issues," *IJESRT*, vol. 2 no. 4, pp. 930-936, 2013.

[31]. M. Allen, M. Iqbal, S. Srirangarajan, H B, Lim, L. Girod and A. J. White, "Real-time in-network distribution system monitoring improve operational efficiency," *Journal AWWA*, , vol. 103, no. 7; pp 63-75, 2011.

[32]. M. Paavola and K. Leivska, Wireless Sensor networks in industrial automation. In Chapter 10 Factory Automation, Intech, 2010

[33]. C. Townsend, S. Arms, MicroStrain, Inc.,"Wireless sensor networks: principles and applications", Chapter 22 in sensor technology handbook by Jon S. Wilson, pp. 575-587, *Elsevier*, 2005

[34]. ISA SP-100. http://www.isa.org/.

[35]. J. Akerberg, M. Gidlund, M. Bjorkman, "Future Research Challenges in Wireless Sensor and Actuator Networks Targeting Industrial Automation," *Proc. of IEEE 9th Int. Conf. on Ind. Informatics (INDIN)*, pp. 410- 415, 2011.

[36]. I. Silva, L.A Guedes, P. Portugal, F. Vasques, "Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications," *Sensors* 2012, 12, pp. 806-838

[37]. S. Toteda, "Wireless Sensor Networks: Implementing Reliable, Simple and Secure Industrial Wireless Solutions," *Proc. of SENSOR &TEST II*, pp. 219-222, 2009.

[38]. P. Radmand, A. Talevski1, S. Petersen and S. Carlsen, "Comparison of Industrial WSN Standards," *4th IEEE Int. Conf. on Digital Ecosystems and Technologies (IEEE DEST 2010)*, pp. 632-637, 2010.

[39]. A Millennial Net White Paper ; Maximizing Data Reliability in Wireless Sensor Networks; http://www.millennialnet.com/MillennialNet/media/Resources_Media/WhitePapers

[40]. S-J Lee, E. M. Belding-Royer and C. E. Perkins, "Scalability study of the ad hoc on-demand distance vector routing protocol," International Journal of Network Management, Volume 3, no. 2, pp. 97-114, 2003.

[41]. S. N. Pakzad, G. L. Fenves, S. Kim; and D. E. Culler, "Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring," *ASCE J. of Infr. Sys.*, vol. 14, no.1, pp. 89-101, 2008

[42]. A.E.A.A. Abdulla, H. Nishiyama, N. Ansari and N. Kato, "HYMN to Improve the Scalability of Wireless Sensor Networks," *in Proc. of 3rd IEEE Int.l Workshop on Wireless Sensors, Actuator and Robot Networks*, pp. 519-524, 2011.

[43]. A. Vecchio, "Adaptability in wireless sensor networks,"in *Proc. of 15th IEEE Int. Conf. on Elect.s, Circuits and Sys. (ICECS)*, pp.1261 – 1264, 2008.

[44]. A. Tufail, "Reliable Latency aware routing for clustered WSNs," *Int. J. of Dist. Sensor Netw*., vol. 2012, Article ID 681273, 6 pages, 2012.

[45]. O. Dousse, P. Mannersalo and P. Thira, "Latency of wireless sensor networks with uncoordinated power saving mechanisms," in *Proc. of the 5th ACM* Int. *Symp. on Mobile ad hoc networking and computing (MobiHoc'04)* , pp. 109-120, 2004.

[46]. K. Shashi Prabh, "Real-Time Wireless Sensor Networks," Ph.D. Thesis, Department of Computer Science, University of Virginia, Charlottesville, VA, USA, 2007.

[47]. P. D. Christofides, J. F. Davis, N. H. El-Farra, D. Clark, K. Harris, and J. N. Gibson, "Smart plant operations: Vision, progress and challenges," AIChE *Journal*, vol. 53, no. 11, pp. 2734–2741, 2007.

[48]. J. N. Al-Karaki, and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Comm.*, vol. 11 , no.6, pp. 6-28,2004.

[49]. P.Park, "Protocol Design for Control Applications using Wireless Sensor Networks,"Licentiate Thesis; KTH, Stockholm, Sweden 2009

[50]. C. Fischione, P. Park, P. Di Marco and K. H.Johansson, "Design Principles of Wireless Sensor NetworksProtocols for Control Applications", chapter in Wireless Network Based Control, *Springer*, 2010.

[51]. J. R. Moyne and D.M. Tilbury, "The Emergence of Industrial Control Networks for Manufacturing Control, Diagnostics, and Safety Data; *Proc. of the IEEE*, vol. 95, no. 1, pp. 29 – 47, 2007.

[52]. A. A. Cardenas, T. Roosta and S. Sastry, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems," *Ad Hoc Networks*, no.7, pp. 1434–1447, 2009.

[53]. H. Zhou, The Internet of Things in the Cloud: A Middleware Perspective, *CRC press-Taylor and Francis*, pp. 153-155, 2013.

[54]. Meshnetics, Meshnetics Demonstrated Integration of Wireless Sensor Data with SCADA System, available at: online at www.meshnetics.com, accessed November 2009.

[55]. R. Roman , J. Lopez and C. Alcaraz "Do Wireless Sensor Networks Need to be Completely Integrated into the Internet?", *Future Internet People, Things Serv. (IoPTS) eco-Syst.*, 2009.

[56]. Arch Rock Homepage. Available from: http://www.archrock.com [October 2008].

[57]. OCTAVEX Wireless Sensor work. http://www.octavetech.com/solutions/octavex.html

[58]. SynapSense OneClick WSN software architecture, http://www.synapsense.com

[59]. J. Shneidman, P. Pietzuch, 1. Ledlie, M. Roussopoulos, M. Seltzer, M.Welsh - Hourglass: An Infrastructure for Connecting Sensor Networks and Applications, *Harvard Technical Report TR-21-04*

[60]. M. Isomura, C. Decker and M. Beigl, "Generic Communication Structure to Integrate Widely Distributed Wireless Sensor Nodes by P2P Technology," *in Proc. of 5th Int. Conf. on Ubiq. Comp. (Ubicomp 2005)*, Tokyo September, 2005.

[61]. M. Isomura, C. Decker, M. Beigl, T. Reidel and H.A.H.H. Horiuchi, "Sharing sensor networks," in *Proc. of the 26th IEEE Int. Conf. Workshops on Distr. Comp. Systems*, Lisboa, Portugal, 2006.

[62]. I. Chatzigiannakis, G. Mylonas and S. Nikoletseas, "50 Ways to Build your Application: A Survey of Middle-Ware and Systems for Wireless Sensor Networks," *IEEE Conf. on Emerging Technologies and Factory Automation*, Greece, pp. 466-473,2007.

[63]. ZigBee Alliance, www.zigbee.org

[64]. HART Field Communication Protocol Specification, Revision 7.0, HART Communication Foundation, Sept. 2007.

[65]. Wireless Systems for Industrial Automation: Process Control and Related Applications, ISA-100.11a-2009 Standard, 2009.

[66]. S. Zats, "Wireless Sensor networks Scaling and Deployment in Industrial Automation," http://robotics.eecs.berkeley.edu/~pister/publications/dissertations/ZatsSamuel_MSReport2010.pdf

[67]. Honeywell, http://honeywell.com

[68]. Emerson Process, http://www.emersonprocess.com

[69]. ABB, http://www.abb.com

[70]. Rockwell, http://ab.rockwellautomation.com.

[71]. Yokogawa, www.yokogawa.com

[72]. S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The Format War Hits the Factory Floor," *Ind. Elect. Mag.*, vol. 5, no. 4, pp. 23-34, 2011.

[73]. M. R. Akhondi, A. Talevski, S. Carlsen and S. Petersen, "Applications of Wireless Sensor Networks in the Oil, Gas and Resources Industries," in *Proc. AINA'10*, April 2010, pp.941-948

[74]. M. Kuorilehto, M. Kohvakka, J. Suhonen, P. Hamalainen, M. Hannikainen, and T. Hamalainen, "Ultra-Low Energy Wireless Sensor Networks in Practice: Theory, Realization and Deployment," Hoboken, NJ: *John Wiley & Sons*, 2007

[75]. K. S Low, WNN Win, M. J. Er, "Wireless sensor networks for industrial environments," *Proc Int Conf Comput Modelling, Control Auto (Vienna, Austria 2*, 28–30 November, 2005.

[76]. M. Cheffena, "Industrial wireless sensor networks: channel modeling and performance evaluation," *EURASIP J. on Wireless Comm and Netw*, 297, 2012.

[77]. A. Willig, K. Matheus, and A. Wolisz, "Wireless technology in industrial networks," *Proc. of the IEEE*, vol. 93, pp. 1130–1151, 2005.

[78]. J. Slipp, Changning Ma, N. Polu, J. Nicholson, M. Murillo, and S. Hussain, "WINTeR: Architecture and Applications of a Wireless Industrial Sensor Network Testbed for Radio-Harsh Environments," In 6th *Annual Conf. on Comm. Networks and Services Research Conf., 2008 (CNSR*), pp. 422 –431, 2008.

[79]. T. O'Donovan ,J. Brown, U. Roedig, , C. J. Sreenan, J. do O´, A Drunkels, A. Klein, J. S. Silva, V. Vassiliou, L. Wolf, " GINSENG: Performance Control in Wireless Sensor Networks," in *Proc. of 7th IEEE Comm. Society Conf. on Sensor mesh and Ad Hoc Comm. and Netw.(SECON)*, pp.1-3, 2010.

[80]. J. Lopez , R. Roman and C. Alcaraz, "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks, Foundations of Security Analysis and Design V," FOSAD 2007/2008/2009 Tutorial Lectures, *Springer-Verlag*, Berlin, Heidelberg, 2009.

[81]. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmoriand Ramjee Prasad, "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach", *Center for TeleInFrastruktur*, Aalborg University.

[82]. J. Akerberg, M. Gidlund, M. Bjorkman, T. Lennvall and J. Neander, " Efficient Intergration of secure critical industrial wireless sensor networks," *EURASIP J. on Wireless Comm. and Netw*, vol. 100, 2011.

[83]. H. J. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," *Int. J. of Dist. Sensor Netw*. Vol. 2012 (2012), Article ID 268478, 10 pages.

[84]. V.L. Priya and C.B. Subramanian, " A proposed architecture for SCADA network security," *Proc. of IEEE Int. Conf. on Computer, Comm. and Elect. Tech. (ICCCET)*, pp. 142-145, 2011.

[85]. J.N. Al-Karaki, R.UI-Mustafa and A.E. Kamal, "Data Aggregation and Routing Routing in Wireless Sensor Networks:Optimal and heuristic algorithms," *Comp. networks*, vol. 53, no. 7, pp. 945-960, 2009.

[86]. C. Chong and S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", *Proc. of the 6th Int. Conf. on Mobile Computing and Networking (Mobicom)*, Boston, USA, pp. 56 - 67, August 2000.

[87]. K. Yu, M. Gidlund, J. A. Akerberg and M. Bjorkman, "Reliable-real time protocol for industrial wireless sensor and actuator networks," in *Proc. of 8th IEEE Int. Conf. on Ind. Elect. and Applications (ICIEA)*, pp.1895-1901, 2013.

