Volume 3, Issue II, Feb. 2024, No. 47, pp. 509-524
Submitted 2/2/2024; Final peer review 21/2/2024
Online Publication 24/2/2024
Available Online at http://www.ijortacs.com

REAL-TIME GUARANTEE: CRITICAL ISSUES IN WIRELESS INDUSTRIAL PROCESS CONTROL-EXPLORING ENHANCEMENT OPTIONS

Dr. Ulagwu-Echeu A.C.
Industrial Project Resources & Operational Supports Ltd. (IPROS LTD)
Corresponding Author Email : aulagwu@yahoo.com;

Abstract

Ensuring real-time data transfer in Wireless Industrial Control System (WICS) networks has been a persistent challenge, marked by issues such as security vulnerabilities, high power consumption, inadequate maintenance, and insufficient monitoring. This research delves into these critical challenges, examining their impact on the quality of service in WICS. The study then explores proposed solutions with the potential to mitigate each of these identified issues. Additionally, the paper provides an overview of control system networks, wireless ICS, and outlines the requirements for integrating wireless networks into ICS. The suggested solutions, along with the outlined integration requirements, are recommended as enhancement options to guarantee real-time performance in control system networks.

Keywords: Industrial Process Control, Wireless, Real-time guarantee, integration

1. INTRODUCTION

Intelligent manufacturing systems are contemporary production systems that combine human, machine, and process capabilities to get the optimum results. Within this framework, industrial system behaviour is directly influenced by control procedures. They are expected to function in a precise, dependable, and safe manner. To guarantee this, several contemporary technologies including artificial intelligence (robotic technology) and wireless networks are incorporated into a single design (Grobelna, 2023).Process control is used to make the process more efficient and to maximize output while preserving the required level of product quality and safety. Process control systems are utilized in facilities that produce chemicals, pulp and paper, metals, food, and

medicines since these objectives apply to a wide range of sectors. Regardless of the scale of the plant, the principles of automated control are generic and may be widely applied, even though production processes vary between industries (Hahn, 2014).A mixture of structures, methods, and algorithms are used in industrial factories for process monitoring and control, which involves keeping an eye on and managing the actions of a certain process to accomplish a particular goal. The majority of process control applications have strict criteria and are mission-essential. In process-controlled facilities, a control loop failure might result in an unplanned plant closure or potentially serious accidents (Zhao, 2011). In both the discrete and process manufacturing sectors, controllers ranging from proportional controllers, and state estimators, to advanced predictive controllers like Model Predictive Control (MPC) (Ulagwu-Echefu et al., 2021a) are frequently used to ensure the stability and efficiency of the production process. Nonetheless, the process of designing these traditional controllers frequently entails a thorough examination of the dynamics of the process, the creation of abstract mathematical models, and ultimately, the derivation of control policies that satisfy specific design requirements (Spielberg et al., 2017).

Because of this, traditional industrial control algorithms frequently have poor performance, high dependence on domain expertise, and limited scalability. Applying data-driven strategies to optimize the policies for industrial process control has been an intriguing field of research due to recent advancements in Artificial Intelligence-Internet of Things (AIIoT) techniques (Ruui et al., 2020). It is hoped that a data-driven control policy, given conditional parameters, can produce optimized control parameters, leading to desired control results, such as improved production quality, increased energy efficiency, and reduced emissions of air pollutants, among other things (Feng and Guan, 2022).There is a lot of promise for consumer, business, and industrial uses for wireless sensor network technologies. In particular, process data may be wirelessly sent from sensing devices to a control system for operation and management. This data includes measurements of pressure, humidity, temperature, flow, level, viscosity, density, and vibration intensity. There are several benefits to using WSNs for process control and monitoring over conventional wired systems (Zhao, 2011).

In the industrial sector, wireless communication for process control is relatively new, mostly due to a lack of confidence in its capabilities. Wireless communication technology has not been regarded as firmed until recently. With the advent of new wireless communication technologies

and protocols such as the Institute of Electrical Electronics Engineering (IEEE) 802.15.4 standard (IEEE, 2015), which is continuously updated, and more potent, energy-efficient, and secure microcontrollers built on the Arm Cortex-M family of processors, the current scenario is a little different (Rusu and Dobra, 2019).**The contribution of the paper**

i. Non-exhaustive literature review on real-time wireless process control systems

ii. Comprehensive overview of industrial process control system and Wireless Industrial Process Control System (WIPCS)

iii. Requirements for the integration of wireless network control system network

iv. Exploration of critical issues in wireless industrial process control and enhancement options

2. LITERATRUE REVIEW

Rusu and Dobra (2019) researched on channel hopping in wireless process control system. The study is aimed at addressing the challenges of lack of robustness and determinism interference and range problem in the wireless process control system using channel hopping technique. The study was implemented on a low-power Arm based micro-controller paired with an IEEE 802.15.4 sub-GHz transceiver. The result of the system reported that the system has a maximum transmit power of -7dBm. Deisy (2015) researched on the use of Radio Frequency (RF) signal on wireless control of industrial process. The study is aimed at the determination of the requirement to transmit character strings of data on an industrial wireless process control system. In the study, the functionality of the process plant is described; process plant which uses RF receiver, process device and the processor like pump, blower can control the pump which is used in the oil industries and Blower which is used to reduce the heat of the heater.The study is a review and the practical implementation of the work was not reported in the study.Zand et al., (2012) presented a study on the journey of wireless industrial monitoring and control networks. The study provides an overview on the wireless technology can be applied for monitoring and control of a process control in an industry. The advantages and disadvantages of these applications are also presented. The mechanisms proposed by academia by addressing the real-time and reliability requirements of the process control industry are also reported in the work. The work concluded by identifying some key research issues that require attention for successful use of wireless

technology in industrial monitoring and control sector. Teffera (2013) presented a study on the process control over wireless sensor networks. This study is an experimental study on the network and controller performance of a wireless sensor network on a process control system. A centralized discrete controller is used in the system for controlling the thermal processes that run on the sensors. The system was implemented using a wide industrial networked control systems while adding a WSN dimension based on IEEE 802.15.4 and Routing Protocol for Low power and Lossy Networks (RPL). The result of the system implementation reported that the system has a maximum theoretical delay of 0.2487seconds.

3. INDUSTRIAL CONTROL SYSTEM NETWORK

Industrial control system (ICS) is an electronic control system which is associated with instrumentation tools for industrial automation process (Kagermann et al., 2013). The ICS consists of control system components such as electrical devices, mechanical system and control systems, that act together to achieve industrial objectives, such as manufacturing, transportation of matter or energy, and product handling. ICSs can range in size from a few modular panel-mounted controllers to large systems with multiple sites and remote access capabilities (Al-Dabbagh and Chen, 2016). The ICS is made up of various types which include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Programmable Automation Controllers (PACs), Remote Terminal Units (RTUs), control servers, intelligent electronic devices (IEDs), and sensors (Park et al., 2018). According to Bello and Zeadally (2016), ICS has three main types of networks which are plant network, control network, and field network as depicted in figure 1.

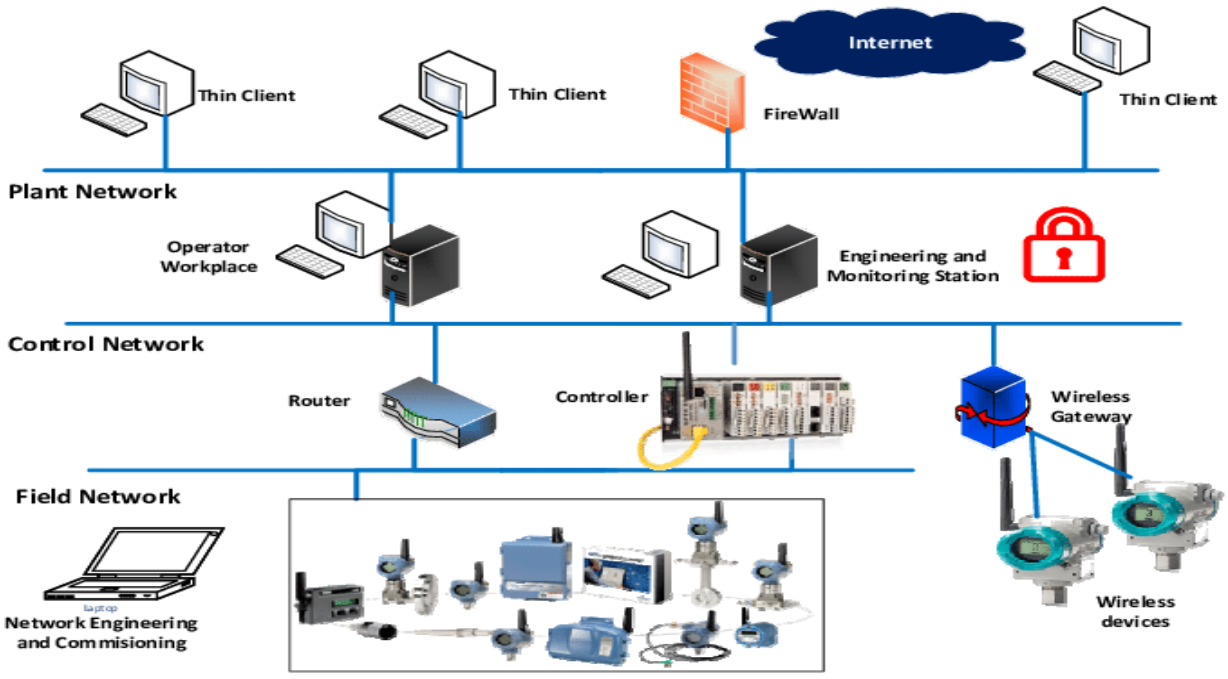

Figure 1: Block diagram of a process control loop (Alford and Buckbee, 2020)

The Figure 1 presents the classification of ICS components in three layers. The plant network layer is a business network that handles enterprise-level data and is typically located at the core layer of the network. The control network is the Process Control Network (PCN) that handles data from PLCs and field devices (Bello and Zeadally, 2016). The field network is the wireless network that connects field devices, such as wireless transmitters, to the control network. When selecting a wireless protocol for the field network, it is important to consider factors such as range, data handling, reliability, latency, and security. WirelessHART and ISA100 are commonly used for process control and monitoring instrumentation, while Wi-Fi and 5G cellular are used for mobile worker and data backhaul. The process design engineer can use a set of criteria to identify wireless application candidates, including safety systems, critical control, on-off control, in-plant monitoring, and remote monitoring Field devices includes sensors, actuators, and instruments, are crucial components of an ICS, located in the Level 0 (Field) layer of the Purdue Reference Model (Sadi et al., 2014). The SCADA system serves as the central hub of control in an ICS, monitoring and controlling industrial processes by collecting data from remote devices and providing real-time data to operators (Sadi et al., 2014). The control loop consists of hardware such as PLCs and actuators, which interpret signals from sensors, control valves, breakers, switches, motors, and other devices (Demir and Ergen, 2016). The ICS also includes

physical networks, such as the Process Control Network (PCN) and the Business Network (BN), which handle data from PLCs and field devices and enterprise-level data handling and communication, respectively. The Figure 1 presents an architectural illustration of ICS which classified the components of the ICS into three main categories of plant network, control network and field networks respectively (Bello and Zeadally, 2016).

4. WIRELESS INDUSTRIAL PROCESS CONTROL (WIPC) SYSTEM

A crucial business enabler in the automation sector is wireless technology. Many industrial outfits have quickly adopted it due to its flexibility, cost-effectiveness, speedy deployment, and dependability. Ultrahigh Frequency (UHF) radios have been widely employed for long-range Supervisory Control and Data Acquisition (SCADA) communication in the power and utility, as well as the oil and gas industries, for the past forty years (Zand et al., 2012). Using 25 kilohertz channels, the UHF radio platform provided the best low-speed communication option for linking field Remote Terminal Units (RTUs) to a central SCADA host. About 19.6 kilobits per second of wireless data rate were obtained. Pulling data from field equipment and transmitting supervisory control commands like closing/opening a valve or starting/stopping a pump to the field is hardly possible with this capability (Soliman, 2022).To meet the demands of modern company operations, high-speed communication via broadband wireless technology has to be used. Adapting SCADA technology keeps using new technologies at various levels, leveraging open standards and cutting-edge innovations to provide integrated services and capabilities over larger domains. Examples of typical information technology/operational technology (IT/OT) integrated services include intelligent field, closed-circuit television (CCTV), mobile radios with video streaming, and field computing applications (Murugamani et al., 2022).

Several wireless backhaul technologies were established to provide certain services, including data communication, video, and voice. As a result, several disparate and heterogeneous wireless systems were deployed. Moreover, only a small number of approved wireless instrumentation devices that meet WirelessHART or ISA-100.11a criteria exist, even though wireless instrumentation standards were established more than five years ago. The automation community's inability to work together to expedite standardization efforts and advance the development of a unified wireless instrumentation protocol was a significant contributing factor. According to Anders et al. (2019), end users were apprehensive about the widespread use of

wireless instrumentation technology due to lack of clarity. These ICS systems are outfitted with wireless transmitters and receivers that can talk to one another and accomplish flawless data exchange and monitoring capabilities. However, the performance of this wireless-based ICS has not yet reached the necessary potential expected for Industry 4.0 due to several factors, including the distance between the plants and monitoring centres in some cases, environmental factors like temperature and harsh weather in specific plant locations like the oil well, mining field, and substation sites, among others (Ulagwu-Echefu et al., 2021b).Based on their coverage area, industrial wireless technologies may be broadly divided into three groups (figure 2) (Soliman, 2022):

i. Wireless connected devices: IPv6, WirelessHART, ZigBee, and ISA-100.11a are the most used protocols over low-power wireless personal area networks (LoWPANs).

ii. Wireless backbone networks as the access point: IEEE 802.11a/b/g/n/ac Wi-Fi family is the industry leader.

iii. Wireless backhauls networks links: dominated by UHF radio and moving towards microwave, satellite (Ka-band VSAT), and 4G long-term evolution (LTE) technologies

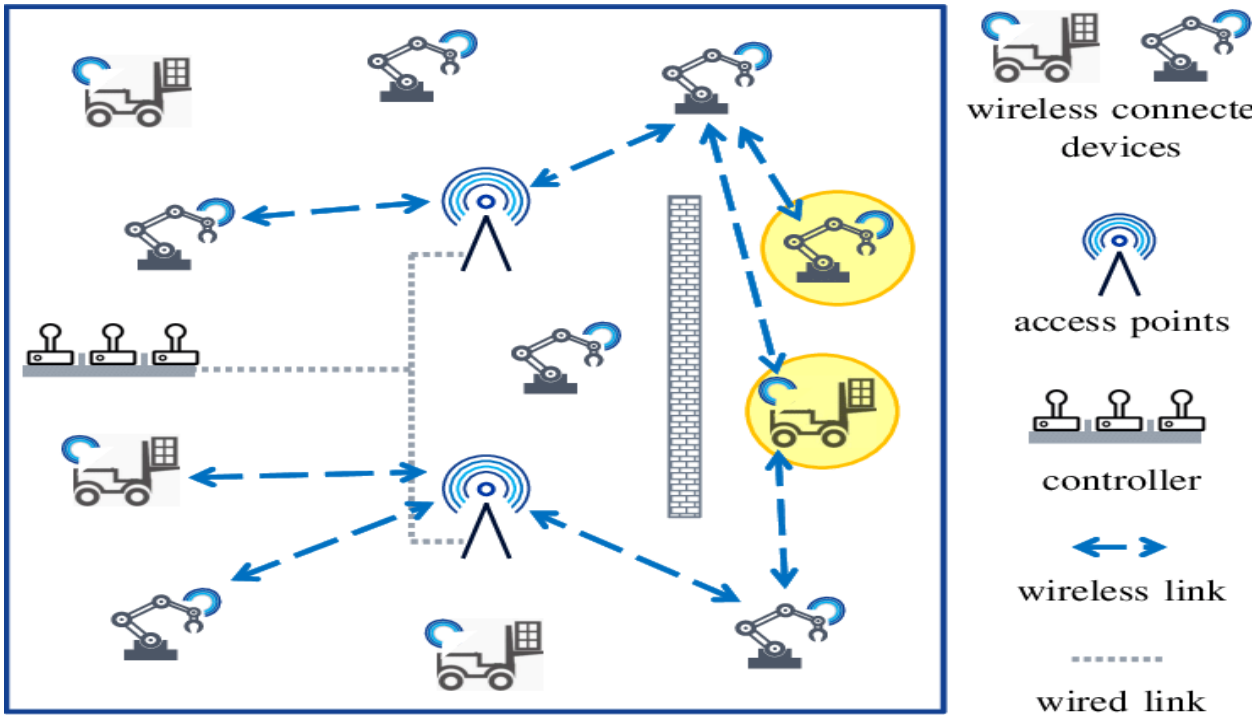

Figure 2: Wireless Industrial Process Control system framework (Zheng, 2010)

5. Requirements for Wireless Industrial Process Control System Integration

Wireless industrial process control systems require careful evaluation of wireless protocols to ensure that they meet specific industrial automation requirements of the system integration. For effective integration of wireless network in ICS, several protocols such as WirelessHART, ISA100, Wi-Fi, LoRa, and 5G are standards existing to facilitate smooth integration of wireless ICS. During the integration process, critical factors which improved channel reliability such as range of components position from the communication device, data handling, reliability, throughput, losses, latency, and security are vital to maintain quality of service during the integration process are also necessary to e considered. Today wireless network application of ICS has continued to expand and is becoming more complex, hence presents the need for enhanced improvement on the standards for integration. While the existing recommendations focused on standardized protocols and channel reliability, however the need for security is also a vital components for wireless network integration on ICS. The figure 3 presented the three main requirements for the integration of wireless network in ICS.

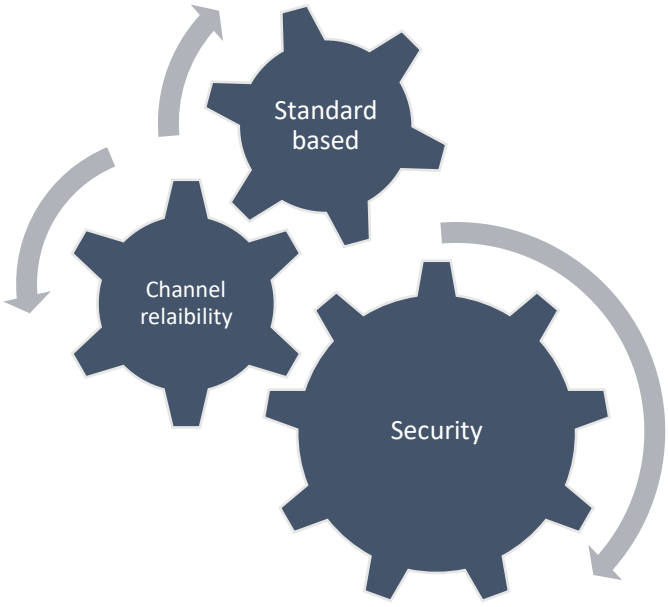

Figure 3: Requirements for WIPC system

a. Channel reliability

An essential prerequisite for automation systems is channel dependability. To identify problems and request retransmission, a basic parity check or cyclic redundancy check was utilised in the past. Spread spectrum, Forward Error Correction (FEC), adaptive code modulation, and intelligent power control mechanisms are examples of technological advancements. These increase channel dependability and offset any attenuation brought on by external buildings or the weather. Furthermore, in the 2.4 and 5 gigahertz (GHz) frequency bands, redundant and dual-frequency transmission is becoming common for plant backbone networks.

b. Security

Since air is a shared medium in the wireless realm, security is one of the fundamental issues. The recommended security criteria for the integrity, confidentiality, and privacy of transmitted data were set by ISA-100.11a and ISA-100.15. Strong mutual authentication and the hardware-based advanced encryption standard (AES-128 bit) are essential security needs.

c. Standard-based

To guarantee interoperability, the ability of wireless components from many manufacturers to work together, standard-based radio is equally crucial. To guarantee that goods adhere to the stated technical criteria and requirements in comparison to the ISA-100.11a standard, the ISA100 Wireless Compliance Institute was founded. Other wireless standardization organizations, such as WirelessHART, ZigBee, Wi-Fi, VSAT (DVB), and LTE, also created certifications and compliance procedures to their specifications.

6. Critical Issues In Wireless Industrial Process Control

Even though using wireless technology for industrial process management has many advantages, there are still a lot of problems and difficulties with the setup. To increase the system's performance, security, and dependability, these problems must be resolved. Among the key problems with wireless industrial process control that are evident are (Jacob, 2022):

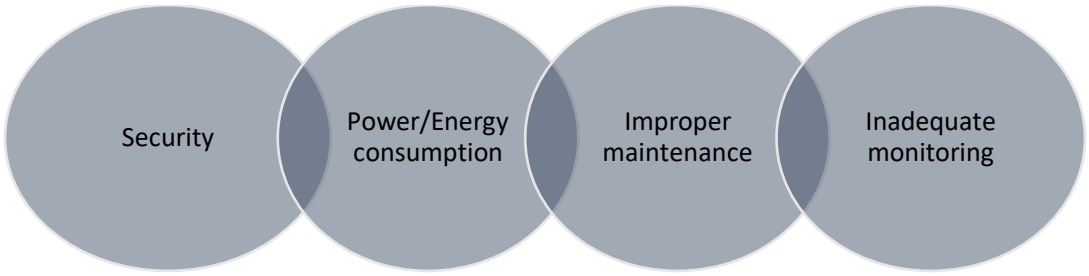

Figure 4: Critical Issues in Wireless Industrial Process Control

a. Security

All sectors and businesses have difficulties related to information security, system security, and cybersecurity. These are particularly pressing issues for the manufacturing industry, particularly about industrial automation control systems (McMorrow, 2023).

There are several risks to industrial automation control systems:

- Targeted external attack to deliberately hinder production
- Targeted external attack to impact the state or quality of the product produced
- Indiscriminate external attack
- Ransomware attacks (extortion)
- Actions by disgruntled employees

Attackers can take advantage of technological weaknesses in systems, just like they do with information systems in other business settings. Illegal access to this network may be both permitted and unauthorised. In the latter instance, attackers typically take advantage of non-technical security flaws in an organisation to obtain unauthorised access to a system. One example is using social engineering tactics to deceive employees.

b. Power/Energy Consumption

Energy consumption for industrial processes is rising. According to recent research examining the energy consumption of manufacturing facilities in the US and Canada, the average manufacturing facility increased its energy usage by 6% in less than two years. What's causing this rise? Even while machinery has been increasingly efficient over time, growing

miniaturisation has allowed businesses to employ a greater number of machines. Furthermore, more devices have computers installed, which use more energy (SAAB, 2022).Industrial businesses therefore have greater energy consumption, and predictions indicate that this tendency will continue. However, energy has stayed so inexpensive for so long that many makers of equipment have chosen to ignore energy efficiency in favour of production or dependability. These inclinations have prepared the way for the industrial sector's energy costs to rise quickly. But this is only a small portion of the larger issue. Macro-market dynamics are also at work, which might make things worse.

c. Improper Maintenance

For most equipment to operate at its best, regular maintenance is necessary, but when you're overworked and understaffed, preventative maintenance frequently gets neglected. When everything seems to be going smoothly, it's simple to ignore routine maintenance, and many businesses operate on the belief that skilled personnel will see potential problems before complete equipment failure (Kaushal et al., 2019).Equipment malfunctions are difficult to identify and frequently go unreported. In other instances, businesses just don't have effective planning techniques in place to guarantee that continuous maintenance is carried out. Using asset tags to track machinery and equipment may assist ensure that maintenance plans are followed and that the gear is running as efficiently as possible. One continuous process that should never be neglected is preventive maintenance. By providing your equipment routine tune-ups, you may increase its useable life and ultimately get more for your money. Preventive maintenance also can spot minor issues and provide low-cost fixes before they worsen and result in expensive failures. Equipment downtime for regular maintenance and repairs is reduced when you employ efficient inventory control techniques to guarantee that you have the appropriate spare parts on hand for the majority of maintenance chores and malfunctions.

d. Inadequate Monitoring

To identify small changes that may be utilised to forecast malfunctions and breakdowns, continuous monitoring depends on sensor data to create a baseline for what optimal equipment condition looks like (Masani et al., 2019). This gives planners more time to prepare for unforeseen events and arrange downtime to reduce disruptions to production. Businesses may detect the reasons for increasing equipment stress and modify workloads and schedules to

prevent asset failure with the use of this kind of monitoring and the data gathered during the process (Goncalves, 2022).

7. Exploring Enhancement Options For The WICS Critical Issues

To address these critical issues in the wireless industrial process control system, a combination of various technical solutions, vigilance and practices are recommended. Some of the solutions considered in this study are presented using the illustration in figure 5;

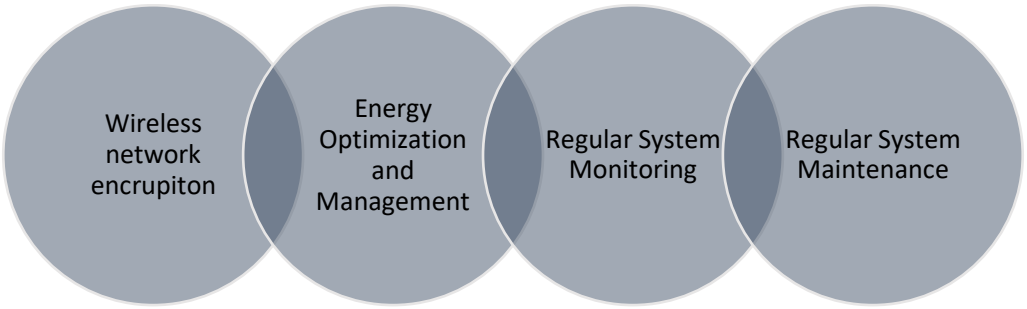

Figure 5: Illustration of the enhancement options for critical WICS challenges

a. Wireless Network Encryption

For industrial WLAN applications, only the Wi-Fi Protected Access 2 (WPA2) security standard with Advanced Encryption Standard (AES)-level encryption is advised. While AES encryption is done at the hardware level and does not impact the speed of an application, WPA2 delivers the most robust security currently available for WLANs in industrial environments (Venkataraman, 2016).WPA2 may enable 802.1X/Extensible Authentication Protocol (EAP) and pre-shared key authentication in an autonomous architecture. Which of these two authentication techniques is best for your autonomous WLAN may be determined by taking into account factors like infrastructure support, implementation convenience, and security policy. To accommodate various client types, you may also decide to employ many authentication techniques in a single autonomous architecture.

b. Energy Optimization and Management

The anticipatory, structured, and methodical coordination of energy acquisition, conversion, distribution, and utilisation to meet needs while accounting for environmental and financial objectives is known as energy management. To handle energy efficiently, the energy

management process entails a variety of activities, including planning, buying, measuring, monitoring, regulating, documenting, and calculating the cost of energy use (El-Abbassi et al., 2015).The ultimate objective of energy management is to maximise production efficiency and economy by controlling and optimising energy consumption. A continuous improvement process (operation sequence), similar to quality management, is required to accomplish this aim at several different levels, including system, process, equipment, and facility levels.

c. Regular System Monitoring

Any automated controlled system's long-term, dependable functioning depends heavily on process monitoring. An unidentified, uncontrollable input operating on a system is called a disturbance. An unapproved divergence of at least one system characteristic property or parameter from the permissible, customary, or normal operating circumstances is referred to as a fault. A failure occurs when a system's capacity to carry out a necessary function under predetermined operating parameters is permanently disrupted. When there are disruptions, traditional control systems are meant to restore regular operations; when there are errors or failures, they are not meant to do so. Fault-tolerant control systems are those that are specifically engineered to accommodate a certain class of defects in the closed-loop system, ideally before the associated defective equipment deteriorating to the point of system failure (Severson et al., 2015).

d. Regular System Maintenance

Process control systems can be kept in excellent operating order and regular maintenance activities may be ensured if the operator has a suitable maintenance manual. An effective maintenance culture can benefit from the following strategy (NiBusiness, 2023):

i. The operator should always make sure the key parts of the system are working correctly. Carry out regular checks on them

ii. The operator should also keep detailed records of all your maintenance activity in a log book. This will help you when dealing with problems that happen often, improve the process control operation and upgrade the equipment when the life span has been exhausted

8. CONCLUSION

This paper presents a review of the critical issues that can be encountered in the operation of a wireless industrial process control system and the approaches that can be adopted for tackling these issues to provide a real-time guarantee of the system's operation. This study started with a comprehensive description of industrial process control and wireless industrial process control systems. In the paper, the critical issues identified from the research with their recommended solutions are security challenges, for this challenge, wireless network encryption was recommended as an approach to solve the problem. Improper power/energy consumption challenge, this study recommends the adoption of energy optimization and management for tackling the specified challenge. Then, poor or inadequate system monitoring and maintenance were another set of challenges identified in the study, to tackle these challenges, the study recommends the adoption of regular system monitoring and system maintenance culture for early prevention or diagnosis of any challenge in the process control system.

9. REFERENCES

Al-Dabbagh A., & Chen T., (2016) Design considerations for wireless networked control systems. IEEE Trans. Ind. Electron., vol. 63, no. 9, pp. 5547–5557, Sep. 2016.

Alford J., & Buckbee G., (2020) Industrial Process Control Systems: A New Approach to Education. 2020 American Institute of Chemical Engineers (AIChE). Industrial Process Control Systems: A New Approach to Education | AIChE Accessed January 2024

Anders A., Johan A., Markus E., Alf J., Takuya I., Karl H., Steffi K., Thomas L., & Henrik S., (2019). Toward Wireless Control in Industrial Process Automation A CASE STUDY AT A PAPER MILL. IEEE CONTROL SYSTEMS MAGAZINE » OCTOBER 2019 Digital Object Identifier 10.1109/M/CS.2019.2925226

Bello O. and Zeadally S., (2016) Intelligent device-to-device communication in the Internet of Things. IEEE Syst. J., vol. 10, no. 3, pp. 1172–1182, Sep. 2016

Chen D., Nixon M., Aneweer T., Shepard R., Burr K., & Mok A., (2014) Wireless Process Control Products from ISA 2004. https://www.researchgate.net/publication/240419390

Demir U., & Ergen S., (2016) ARIMA-based time variation model for beneath the chassis UWB channel. EURASIP J. Wireless Commun. Netw., vol. 178, pp. 1–11, Dec. 2016

Deisy T., (2015) Wireless Control Of Industrial Process Using RF Signal. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 6103-6111 © Research India Publications

Dunn W., (2005) Fundamentals of Industrial Instrumentation and Process Control. The McGraw-Hill Companies, Inc. http://dx.doi.org/10.1036/0071466932

Feng C., & Guan J., (2022) Reliable Offline Model-based Optimization for Industrial Process Control. arXiv:2205.07250v1 [cs.LG] 15 May 2022.

Goncalves T., (2022) 5 causes of equipment failure (and how to prevent them). (1) New Messages! (fiixsoftware.com) Accessed January 2024

Grobelna I., (2023) Intelligent Industrial Process Control Systems. Sensors 2023, 23, 6838. https://doi.org/10.3390/s23156838

Hahn J., (2014) Process Control. Kirk-Othmer Encyclopedia of Chemical Technology. Copyright John Wiley & Sons, Inc.

IEEE Std 802.15.(2015) IEEE Standard for Low-Rate Wireless Networks Amendment to IEEE std 802.15.4-2011, 2015

Jacob R., (2022) Challenges and recent advances in the design of real-time wireless Cyber-Physical Systems. BenchCouncil Transactions on Benchmarks, Standards and Evaluations. https://doi.org/10.1016/j.tbench.2022.100036

Kagermann H., Wahlster W., and Helbig J., (2013) Recommendations for implementing the strategic initiative industrie 4.0. Forschungsunion Acatech, Frankfurt, Germany, Rep., 2013

Masani I., Oza P., & Agrawal S., (2019) Predictive Maintenance And Monitoring Of Industrial Machine Using Machine Learning. Scalable Computing: Practice and Experience Volume 20, Number 4, pp. 663–667. http://www.scpe.org DOI 10.12694/scpe.v20i4.1585 ISSN 1895-1767 c 2019 SCPE

McMorrow D., (2023) Security Challenges of Industrial Automation Control Systems. Security Challenges of Industrial Automation Control Systems - SL Controls Accessed January 2024

Murugamani C., Sahoo S., Kshirsagar P., Prathap B., Islam S., Naveed Q., Hussain M., Hung B., & Teressa D., (2022) Wireless Communication for Robotic Process Automation Using Machine Learning Technique. Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 4723138, 12 pages https://doi.org/10.1155/2022/4723138

NiBusiness Info (2023) Process control systems for energy efficiency: Maintaining process control systems. Maintaining process control systems | nibusinessinfo.co.uk Accessed January 2024.

Park P., Ergen S., Fischione C., Lu C., & Johansson K., (2018) Wireless Network Design for Control Systems: A Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 2, SECOND QUARTER 2018

Rui N., Jinfeng L., & Biao H., (2020) A review on reinforcement learning: Introduction and applications in industrial process control. Computers & Chemical Engineering 139 (2020), 106886.

Rusu A., & Dobra P., (2019) Channel Hopping in Wireless Process Control. 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC).

SAAB RDS (2022) Industrial Automation: Addressing Rising Power Consumption. Industrial Automation and Power Consumption - SAAB RDS Accessed January 2024

Sadi Y., Ergen S., and Park P., (2014) Minimum energy data transmission for wireless networked control systems. IEEE Trans. Wireless Commun., vol. 13, no. 4, pp. 2163–2175, Apr. 2014.

Severson K., Chaiwatanodom P., & Braatz R., (2015) Perspectives on process monitoring of industrial systems. IFAC-PapersOnLine 48-21 (2015) 931–939 International Federation of Automatic Control. 10.1016/j.ifacol.2015.09.646

Soliman A., (2022) What is the next Generation of Process automation wireless technology? Interchange What Is the Next Generation of Process Automation Wireless Technology? (isa.org) Accessed 2024

Spielberg S., Gopaluni R., & Loewen P. (2017) Deep reinforcement learning approaches for process control. In 2017 6th international symposium on advanced control of industrial processes (AdCONIP). IEEE, 201–206.

Teffera Z., (2013) Process Control over Wireless Sensor Networks. Stockholm, Sweden 2013 XR-EE-RT 2013:025

Ulagwu-Echefu A., Eneh I., & Chidiebere U., (2021a) Enhancing Realtime Supervision and Control of Industrial Processes over Wireless Network Architecture Using Model Predictive Controller. International Journal of Research and Innovation in Applied Science (IJRIAS) |Volume VI, Issue IX, September 2021|ISSN 2454-6194

Ulagwu-Echefu A., Eneh I., & Chidiebere U., (2021b) Mitigating the Effect of Latency Constraints on Industrial Process Control Monitoring Over Wireless Using Predictive Approach. International Journal of Research and Innovation in Applied Science (IJRIAS) |Volume VI, Issue XI, November 2021|ISSN 2454-6194

Venkataraman D., (2016) Securing Industrial Wireless Networks. Rockwell Automation Securing Industrial Wireless Networks (automation.com) Accessed January 2024

Zand P., Chatterjea S., Das K., & Havinga P., (2012) Wireless Industrial Monitoring and Control Networks: The Journey So Far and the Road Ahead. Journal of Sensor and Actuator Networks ISSN 2224-2708 www.mdpi.com/journal/jsan/ 123-152; doi:10.3390/jsan1020123

Zhao G., (2011) Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey. Network Protocols and Algorithms ISSN 1943-3581 2011, Vol. 3, No. 1

Zheng L., (2010) Industrial wireless sensor networks and standardizations: The trend of wireless sensor networks for process automation, Proceedings of SICE Annual Conference 2010, Taipei, Taiwan, 2010, pp. 1187-1190.