4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010)

Comparison of Industrial WSN Standards

Pedram Radmand[1], Alex Talevski[1], Stig Petersen[2] and Simon Carlsen[3]

[1]DEBII, Curtin University of Technology, Perth, Australia
Pedram.Radmand@student.curtin.edu.au, A.Talevski@curtin.edu.au

[2]SINTEF ICT, Trondheim, Norway
stig.petersen@sintef.no

[3]Statoil ASA, Trondheim, Norway
SCAR@StatoilHydro.com

Abstract— **This paper presents a comparison of the current Wireless Sensor Network (WSN) standards that are available for industrial applications. Zigbee, WirelessHART and the recently released ISA.100 are carefully considered. The comparison outlines how WirelessHART and ISA.100 address some of the ZigBee weaknesses in the oil and gas domain.**

I. Introduction

An accelerating energy crisis in the oil and gas industry is driving the development and investment in Wireless Sensor Network (WSN) technologies. WSN is a key investment area across the whole oil and gas supply chain including refineries, petrochemical plants, pipelines, exploration, production, and transportation. By providing secure and reliable two-way wireless communications, WSN enables automation and control solutions that are not feasible with wired systems to improve production, operational efficiency, safety, and asset management[1].

Wireless Sensor Networks (WSNs) comprise of a large number of spatially distributed autonomous devices that may collect data using a wireless medium. They may be used to cooperatively control and monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [2]. WSNs exhibit several unique properties as compared to their wired counterparts such as large scale of deployment, mobility of nodes, temporary installations, redundancy, and dynamic network topologies. However, each sensor node has constraints on operational environment, energy, memory, computation speed and bandwidth [2].

International standards for wireless devices and networks, such as ZigBee, WirelessHART and ISA100.11a use stacks to provide a layered and abstract description of the network protocol design. Each layer in the stack is a collection of related functions, and each layer is responsible for providing services to the layer above it, while receiving services from the layer below it [3].

II. Industrial Requirements

As a result of the strict regulations associated with the installation of wired sensors on oil and gas platforms, the introduction of such devices is complicated, time-consuming and expensive. The primary use cases for WSN in the oil and gas industries are associated with the integration of new sensors and strategies within existing end-of-lifecycle platforms while reducing complexity, time and costs. We have developed the following requirements for the industrial application of WSNs.

A. Reliability

Reliability is a measure of the percentage of accurate data which reaches its destination. This usually is the gateway. Reliability is often used in conjunction with stability. It represents the percentage of successfully transmitted data packets in the network on an individual link basis (the measurement of loss packet). The transfer of data in IEEE 802.15.4 is acknowledge-based (ACK). The transmitter expects to receive an ACK from the receiver for each transmitted packet. The packet is transmitted, if the ACK is not received within a certain time. It is often possible to achieve 100% reliability with no lost packets along with 90% stability through the use of packet retransmission [4].

B. Latency

Latency 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. In fact, there are several factors which effect on latency such as the link quality, which commonly relates to the signal-to-noise ratio in the RF (Radio Frequency) domain. A poor link increases the number of retransmissions and latency. Also, hop-count is another factor which increases latency.

In an IEEE 802.15.4-based full mesh sensor network every sensor is defined as a (FFD) full-function device. For instance, each sensor can work as a sensor unit and a routing device to forward from adjacent sensors toward the gateway [5].

C. Sensor Data Update Rates

As the update rate of the sensor data affects power consumption, a trade-off between update rate and sensor battery life is required. For example, the update rate for temperature data may be 30 seconds for temperature data [5].

D. Wireless Transmission Range

All flow lines on the process deck should be within radio range of one wireless gateway. According to Statoil, studying the proposed individual placements of the sensors showed a radio range of approximately 25 meters is required[5].

E. Power Consumption

There are many factors which affect the power consumption of a wireless sensor node:

- Update Rate: The number of transmissions per time unit increases the rate of power consumption.
- Routing Activity: A sensor node which transmits more packets consumes more energy due to forwarding packets from remote sensors [5].
- Link Quality: Packet transmission in the network is ACK-based. Therefore, a poor link quality, which needs more retransmission, increases the power consumption.

Low power consumption is required to lengthen the intervals between battery replacements as much as possible. The general requirement is a battery life-time of five years at a once per minute update rate [5].

F. Integration with PCDA System

To achieve efficient oil rig application, real-time wireless control and monitoring of platform and well performance is required. These systems are integrated with the plants existing PCDA system. This system is able to integrate sensor data with existing graphical views and monitor the sensor node remaining battery life. Using these data streams production is optimised while minimising safety concerns.

III. Wireless Standards

Several standards are currently ratified for wireless sensor networks. In addition to the standards, there are also several non-standard, proprietary mechanisms and specifications around.

A. Zigbee

The ZigBee Alliance is a group of companies that develop and maintain the ZigBee standard. ZigBee is a specification for a suite of high level communication protocols using low-power digital radios based on IEEE 802.15.4. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other consumer WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking. The low cost allows the technology to be widely deployed in wireless control and monitoring applications .

1) Basic Features

ZigBee is a specification for the higher protocol layer, and builds upon the physical (PHY) and medium-access control (MAC) layers in the 802.15.4 specification.

The protocol is based on the ad-hoc on-demand distance vector (AODV) algorithm. This means, routing, discovery, and peer-to-peer communication is possible through this routing protocol [16]. Mesh networking topologies are supported. All nodes share the same channel and frequency hopping is not available [15].

There are two classes of network devices in ZigBee standards such as Full-Function Devices (FFD) and Reduced-Function Devices (RFD). FFD can form networks of any desired type such as mesh, star and hybrid whereas; RFD can only connect to a full function node [15].

ZigBee can operate in both beaconed and non-beaconed mode. In beaconed mode, the nodes are synchronized and the superframe is divided into 16 slots. There is an option to use up to seven of these as dedicated slots to specific nodes to increase determinism, which is called Guaranteed Slot Time (GTS) [15].

2) Protocol Devices

- **Coordinator -** This device starts and controls the network. The coordinator stores information about the network, which includes acting as a Trust Centre and being the repository for security keys [22] .
- **Router -** These devices extend network area coverage, dynamically route around obstacles, and provide backup routes in case of network congestion or device failure. They can connect to the coordinator and other routers, and also support child devices [22] .
- **End Devices -** These devices can transmit or receive a message, but cannot perform any routing operations. They must be connected to either the coordinator or a router, and do not support child devices [22] .

3) Security

Support for authentication, integrity and encryptions are available, but security is not mandatory. ZigBee makes use of the security mechanisms in 802.15.4; Counter with CBC-MAC (CCM) with AES-128 encryption along with the option to employ encryption-only or integrity-only. However, MAC layer security is not explicitly addressed through the 802.15.4 [17]. Three key types are applied in Zigbee security mechanism: Master key, Link key and Network key. The master key is necessary to join the network. The link key is used for end-to-end encryption and provides the highest level of security at the price of higher storage requirements.

The network key is shared between all devices, and provides a lower level of security. The Network key brings the benefit of reduced storage requirements in devices. All keys can be set in trust centre or coordinator. In fact, the trust centre can control the joining of new devices and periodically update the network key [17]. It should be mentioned that Replay

attacks is protected by using sequential numbering techniques [15].

B. WirelessHART

WirelessHART is a mesh networking technology operating in the 2.4GHz ISM radio band. It utilizes IEEE 802.15.4 compatible DSSS radios with channel hopping on a packet by packet basis. WirelessHART is backward compatible with core HART technology .

Communication is performed using Time Division Multiple Access (TDMA) technology to arbitrate and coordinate communications between network devices. The TDMA Data Link Layer establishes links specifying the timeslot and frequency to be used for communication between devices [18]. These links are organized into superframe that periodically repeats to support both cyclic and acyclic communication traffic. A link may be dedicated or shared to allow elastic utilization of communications bandwidth to assure process data with minimal latency.

1) Basic Features

WirelessHART coexists in the shared 2.4GHz ISM band: Frequency Hopping Spread Spectrum (FHSS), which allows WirelessHART to hop across the 16 channels that are defined in the IEEE802.15.4 standard. CCA (Clear Channel Assessment) is an optional feature in WirelessHART and can be performed before transmitting a message [18]. Moreover, WirelessHART has another feature called transmit power. This feature disallows the use of certain channels, called Blacklisting. These features ensure WirelessHART does not interfere with other co-existing wireless systems, which have real-time constraints [15].

All WirelessHART devices have routing capability and can be treated equally in terms of networking capability, installation, formation, and expansion [15].

There are two different routing protocols in WirelessHART such as Graph routing and Source routing. Graph routing uses pre-determined paths to route a message from a source to a destination device.

Source routing employs ad-hoc created routes for the messages without providing any path diversity. This routing protocol is applied for network diagnostics, and not process related messages [19].

2) Protocol Devices

The following are key components of WirelessHART;

- **Gateway -** Provides the connection to the host network. WirelessHART and the main host are interfaced using Modbus – Profibus – Ethernet. The Gateway also provides the network and security manager [20].
- **Network Manager -** Builds and maintains the mesh network. It identifies the best paths and manages distribution of slot time access (WirelessHART divides each second into 10msec slots) Slot access depends upon the required process value refresh rate and other access [20] .
- **Security Manager -** Distributes security encryption keys. It also holds the list of authorized devices to join the network [20] .

The Process includes measuring devices – the HART-enabled instrumentation.

- **Repeater -** Routes WirelessHART messages but may have no process connection of its own. Its main use would be to extend the range of a WirelessHART network. All instruments in a WirelessHART network have routing capability [21] .
- **Adapter -** Plugs into an existing HART-enabled instrument to pass the instrument data through a WirelessHART network to the host. The adapter could be located anywhere along the instrument 4-20mA cable; it could be battery powered or obtain its power from the 4-20Ma cable. Some adapters will be battery powered and use the same battery to power the instrument as well [21].
- **Terminal -** Used to join a new instrument to an existing WirelessHART network. The terminal has a connection to the gateway and then down to an instrument that can be used for diagnostics [21] .

3) Security

Security is mandatory in WirelessHART. WirelessHART provides end-to-end and hop-to-hop security measures data encryption and message authentication on the Network and Data-link layers. AES-128 block cipher symmetric keys is using for the message authentication and encryption [15].

There are set of security key to ensure secure communication. A new device is provisioned by a join key before each device joins the network. The actual key generation and management are implemented by the Security manager and also Session and Network keys are provided by Network manager for further communication [15].

A Session key is used by the Network layer to authenticate the end-to-end communication between two devices. A Session key is applied for each pairwise communication.

The Data Link layer uses a Network key to authenticate messages on a one-hop basis [15].

C. ISA.100

ISA-100 is the brainchild of the Instrumentation, Systems, and Automation Society (ISA). This standard aims to enable a single, integrated wireless infrastructure platform for plants and delivers a family of standards defining wireless systems for industrial automation and control applications [30]. The ISA 100 standard adheres to a comprehensive coexistence strategy, which provides "the ability of wireless networks to perform their tasks in an environment where there are other wireless networks that may or may not be based on the same standard"[31] .

1) Basic Features

The architecture supports wireless systems that span the physical range from a single, small and isolated network; the

network may include many thousands of devices and multiple networks that can cover a multi-square-km plant [30].

The protocols in ISA.100 have capabilities to reserve for future use and version numbers in headers that allow future revisions to offer additional or enhanced functionality [30].

ISA.100 standard supports channel hopping to avoid any interference from other RF devices operating in the same band and provides the robustness to mitigate multipath interference. Moreover, this standard facilitates coexistence with other RF systems along with the use of adaptive channel hopping to detect occupied channels and/or those with poor performance [30].

Like WirelessHART, this standard, defines TDMA mechanism, which allows a device to access the RF medium without having to wait for other devices [30].

ISA.100 is fully redundant and self-healing and supports end-to-end network reliability [30].

This standard differs from other standards and the network layer uses header formats to be compatible with the IETF (Internet Engineering Task Forces) 6LoWPAN standard to facilitate potential use of 6LoWPAN networks as a backbone. It should be mentioned that by using this standard, the headers compatible with 6LoWPAN does need to be based on the Internet Protocol (IP).

Furthermore, the use of header formats based on 6LoWPAN and IP does not imply that a network based on this standard is open to internet hacking; in fact, networks based on this standard, devices will typically not even be connected to the Internet [30].

2) Security

The security services in ISA 100 are selected by policy. The policy is distributed with each cryptographic material, permitting focused policy application. Since a single key is used at a time at the Data Link, except for a brief period of the key handover, the entire sub-network is subject to the same policies at the Data Link [23]. The security manager controls the policies for all the cryptographic materials it generates.

One of the most important factors in the ISA 100 standard is to provide security mechanisms for Single Security System Management for the automation industry. ISA 100 provides simple, flexible, and scalable security that addresses major industrial threats by leveraging 802.15.4-2006 security [24].

Security is a major design facet of ISA100.11a that considers the entire WSN life cycle that includes configuration, operation and maintenance. Security is considered throughout the whole system not only at the PHY layer or MAC sub-layer. This standard allows for reduced costs and quicker implementations [24].

Types of keys using in ISA100 are both symmetrical and asymmetrical key variants. Session keys have a limited lifetime and are updated periodically, which is initiated by a device, to ensure that the session is kept alive. The key update process may be initiated by a device, although it should be pushed from the security manager between the soft and hard lifetime of a session key [25].

IV. Comparison of Wireless Sensor Standard

ZigbeePRO and WirelessHART represent proven industry WSN technologies. However, ISA100 is an emerging technology which promises many new features. This section presents a comparison of these standards from the perspective of basic features and security.

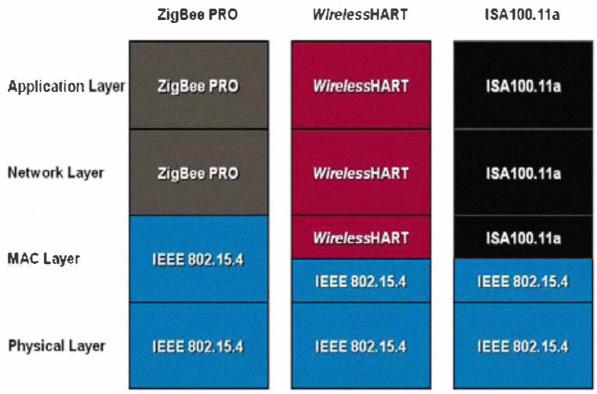

Figure 1: Overall Schema of Wireless Standards [34].

There are some similarities and dissimilarities between WSN standards. All standards are based on IEEE 802.15.4 standards and the same frequency, which is 2.4 GHz. The WirelessHART, like ISA 100, supports mesh, star and combination of mesh and star topology, while Zigbee supports mesh, star and tree topologies. Three standards follow common objectives, such as: interoperability with other communication systems, scalability, energy-saving, communication reliability, compatibility with existing industrial devices, and security [32].

In the industrial market, the International Society of Automation's new ISA100a wireless standard is going to be a threat to ZigBee's future. ISA 100 is able to communicate simultaneously with most popular wired protocols and it can be easily integrated with other wired protocols while Zigbee doesn't support wired protocols. Furthermore, like WirelessHART, the ISA 100 standard incorporates several strategies that are used simultaneously to optimize coexistence with other users of the 2.4 GHz radio spectrum [32].

Like WirelessHART, ISA100 is based on the PHY layer specified in IEEE 802.15.4 but it specifies new Data-link (including MAC), Network, Transport, and Application layers, whereas ZigBee is a specification for the higher protocol layers only. It builds upon the Physical (PHY) and Medium-Access Control (MAC) layers in the 802.15.4 specification [15].

The Application Sub-Layer in ISA 100a is necessary. This promotes interoperability and it is a unique feature of the ISA100 specification that provides a set of common functions available to all applications. The Application Sub-Layer in ISA100a allows different applications in the Application Layer to communicate with each other in different stack layers through a common interface [33]. Table 1 illustrates the summary of features of these three standards:

TABLE1 : WIRELESS SENSOR NETWORK STANDARDS COMPARISON.

Feature Set	Zigbee PRO	WirelessHART	ISA 100.11a
Topology	Mesh	Mesh, Star, Combined Mesh and Star	Mesh, Star, Combined Mesh and Star
Scalability	Yes	Yes	Yes
Radio Channel	CSMA-CD	TDMA	TDMA/ CSMA
RF Channel Change	Yes	Yes	Yes
High Security	Yes	Yes	Yes
Keys	Symmetric	Symmetric	Symmetric/ Asymmetric
Interface Control/ Noise	Yes	Yes	Yes
Energy Saving	Yes	Yes	Yes
Interoperability to other systems	Yes	Yes	Yes
Application Context	Commercial	Industrial	Industrial
Reliability Determinism	No	Yes	Yes
Latency determinism	No	Yes	Yes
Implementation	Easy	Challenging	Challenging

Most standards include protection against jamming and Denial of Service attacks through the use of frequency hopping techniques. As it is mentioned before, all protocols provide secure communication channels to assure the confidentiality, integrity, and authentication of data. However, it is still possible to include a malicious node inside the network to hinder the provisioning of services, but any effects of attacks perpetrated by malicious outsiders can be avoided and mitigated through the security schemas in these standards.

It should be mentioned that WirelessHART and ISA100 have tamper resistance package due to the critically of the environment. As any insider attacks can interrupt the functionality of the network, so the protocols should incorporate with some lightweight security mechanism as well as support for self-healing and intrusion detection system would be significantly useful. WirelessHART already provides support for self-healing. Applying security schema and Public Key Cryptography (PKC) to establish the security infrastructure is a challenge in these standards, but that would be extremely useful for industry.

However, it should be mentioned that applying security schema is the only challenge in such network but network design and users and other factors such as existing connections between the context of the application, its security requirements, and the security mechanisms.

V. CONCLUSION

This paper presented different wireless sensor standards such as Zigbee, WirelessHART and ISA.100, which is recently released industrial wireless network standard and is interesting for industrial applications. The comparison shows that WirelessHART and ISA.100 addressed many of the ZigBee weaknesses and also indicated that WirelessHART and ISA.100 are more suitable for industry applications. The ISA.100, like WirelessHART standard, specifies the communication stack, as well as the interfaces and responsibilities for the various devices comprising an ISA.100 network. Also, it should be mentioned that all the standards protect the communication channel against external attackers, and the refresh keys in the network is provided through specific mechanism.

VI. REFERENCES

[1] M. G. Hatler, D. Chi, Ch., "Wireless Sensor Networks for Oil & Gas." vol. 2010, 2008.

[2] J. Zhang and V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks," in *IEEE Global Telecommunications Conference*, 2008, pp. 1-5.

[3] "WSN Security Project Overview and Scope-Internal Statoil Document " Statoil 2009.

[4] International Electrotechnical Commission, "“IEC 60079- 4: Electrical apparatus for explosive gas atmospheres –Part 4: Method of test for ignition temperature," 1995.

[5] S. S. Carlsen, A. Petersen, S. Doyle, P., "Using wireless sensor networks to enable increased oil recovery," in *ETFA* 2008, pp.:1039 - 1048.

[6] T. S. Lennvall, S.; Hekland, F., "A comparison of WirelessHART and ZigBee for industrial applications," in *WFCS*, 2008, pp. 85 - 88

[7] "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks 2008.

[8] "HART Communication Foundation," http://www.hartcomm.org/index.html, 2007.

[9] "ISA100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.

[10] "ISA100.11a Release 1 Status," ISA 2008.

[11] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments," Lawrence Livermore National Laboratory, April 2007.

[12] "IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), pp. 0_1-305, 2006.

[13] "Looking Ahead: ISA100 Heads to China," ISA, Mar. 2008.

[14] "ZigBee Alliance to Incorporate IETF IT into Wireless Network Standards." vol. 2009: IHS, May 10. 2009.

[15] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of WirelessHART and ZigBee for industrial applications," in Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on, 2008, pp. 85-88.

[16] S. Tian-Wen and Y. Chu-Sing, "A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks," in *Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on*, 2008, pp. 495-500.

[17] S. Jing and Z. Xiaofen, "Study of ZigBee Wireless Mesh Networks," in *Hybrid Intelligent Systems, 2009. HIS '09. Ninth International Conference on*, 2009, pp. 264-267.

[18] D. Wenliang, D. Jing, Y. S. Han, C. Shigang, and P. K. Varshney, "A key management scheme for wireless sensor networks using

deployment knowledge," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 2004, p. 597.

[19] A. K. D. C. L. Jianping Song; Song Han; Mok, M.; Nixon, M., "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control," in *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS '08. IEEE*, 2008, pp. 377 - 386.

[20] "HART Communication Foundation," http://www.hartcomm.org/index.html, 2007.

[21] "The Components of WirelessHART Technology ": HART Communication Foundation, 2009.

[22] "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks, Feb 2008.

[23] "ISA100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.

[24] "ISA-100.11a-2009 Wireless systems for industrial automation: Process control and related applications," ISA, 2009.

[25] D. Sexton, "Understanding the unique nature of the universal family of ISA100 Wireless Standards," ISA Aug. 28 2007.

[26] "IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003),* pp. 0_1-305, 2006.

[27] "Looking Ahead: ISA100 Heads to China," ISA, Mar. 2008.

[28] "ZigBee Alliance to Incorporate IETF IT into Wireless Network Standards." vol. 2009: IHS, May 10. 2009.

[29] L. E. Bassham, "The Keyed-Hash Message Authentication Code Validation System (HMACVS)," December 3, 2004.

[30] "ISA100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.

[31] "ISA100.11a Release 1 Status," ISA 2008.

[32] "ZigBee Alliance to Incorporate IETF IT into Wireless Network Standards." vol. 2009: IHS, May 10. 2009.

[33] "Looking Ahead: ISA100 Heads to China," ISA, Mar. 2008.

[34] K. Masica, "Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments," Lawrence Livermore National Laboratory, April 2007.