Experiences and Future Developments of Wireless Safety Equipment

Adne Baer-Olsen
BDM Dræger GasSecure
Dräger Safety AG & Co.KGaA
Dubai Healthcare City
Building 25, 5th floor
P.O. Box 505108
Dubai
UAE

Tel +971 4 4294 631
Fax +971 4 4294 699

Christian Heinlein
Product Manager
GasSecure AS
Hoffsveien 70 C
0377 Oslo
Norway

Phone: +47 995 95 939

Jørgen Svare
Head of Operations
GasSecure AS
Hoffsveien 70 C
0377 Oslo
Norway

Phone: +47 995 95 939

ACKNOWLEDGMENTS

ISA and WCI for providing information of the matter subject. End users for giving valuable input.

REFERENCES

EP06-3405-ISA100-Wireless-Systems-for-the-Future-brochure-WEB_9-18-14

Adoption-of-Wireless-for-Safety-2016-06-29-Werb

EP06-3405-ISA100-Wireless-Systems-for-the-Future-brochure-WEB_9-18-14

Evolution of Wireless Sensor Networks for Industrial Control

ABSTRACT AND KEYWORDS

Objectives of the paper:
Demonstrate with examples why ISA 100 is the preferred communication for wireless safety.
Description of how to ensure the wireless signal is as safe, or safer, than a wired signal
Describe and present experiences gathered using wireless devices in safety applications.
Present findings that give end users increased safety while reducing cost and increasing flexibility for the end user.
Description of devices available today and various future market developments.

Key words:
- Wireless
- Wireless Safety
- ISA 100
- Cost saving
- Increased flexibility
- SIL

2.0 FINDING THE RIGHT PROTOCOL

Starting to use wireless as part of a safety application gives some stringent requirements to the wireless sensor network responsible for communication. In the marketplace today there are 2 distinct wireless sensor networks available for industrial control; Wireless HART and ISA100.11a.
Comparing the different protocols in the light of safety critical application and data safety the ISA100.11a gives a latency consistent with the requirements for safety application which is a response time in seconds rather than minutes. Data safety can also be demonstrated to be highest in the ISA100.11a protocol, this according to Arthur Low; *Evolution of wireless sensor networks for industrial control*.

2.1 INTRODUCTION TO ISA 100

In 2005 the International Society of Automation (ISA) formed the ISA100 Committee to establish standards, recommended practices, and technical reports to define technologies and procedures for implementing wireless systems in industrial automation and control applications. The wireless standard ISA100.11a (commonly referred to as ISA100) is the first project in the ISA100 family and was first released in 2009. A revised version of this standard was published in 2011 which addressed minor faults and errors in the initial specification.
The ISA100 Committee's standards development processes are open, meaning professionals from more than 250 companies across the industry - suppliers, end users, and other stakeholders - collaborate to craft a wireless standard that meets and exceeds user requirements. In other words, the ISA100 Wireless standard is designed by the industry and for the industry. It is intended to provide reliable and secure wireless operation for safety, control, and monitoring applications.

2.2 DETAILS OF ISA 100 DESIGN

The ISA100 Wireless standard defines the protocol stack, system management, gateway, and security specifications for low data rate wireless connectivity with fixed, portable, and moving field devices supporting very limited power consumption requirements.

2.2.1 Description of the communication stack

The communication protocol stack defines a set of layers, where each layer is a collection of related functions. A layer offers services to the layer above it, and uses services from the layer below. The most common communication stack model is the seven-layered OSI (Open Systems Interconnection) model. The implementation of the seven layers in ISA100 Wireless is illustrated in brief in Table 1.
The physical layer in the ISA100 Wireless standard is based on the IEEE 802.15.4 standard using the 2.4 GHz band. This band is divided into 27 channels each 2 MHz wide and separated by 5 MHz. All of these channels may be used for ISA100 Wireless communication subject to local regulations, *eg.* channel 26 is not permitted for use by FCC in the US).
The ISA100 Wireless standard distinguishes between field devices, for example sensors, valves or actuators, and infrastructure devices *ie.* devices that handle communication to other network devices and the backbone network. For both device groups a number of roles are defined. For field devices the two most important

roles are a) Input / Output (I/O) and b) Router. A field device with a Router role (a repeater) can forward messages wirelessly. The router role is commonly combined with the I/O role, and many field devices including the GasSecure GS01 ISA wireless gas detector are capable of routing messages on behalf of their neighbors.
For infrastructure devices, the most important roles are c) System Manager, d) Backbone Router / Access Point, and e) Gateway.
Refer to Table 1:

OSI Layer	**Function**	**Technology**
Application	Interface with software applications that implement a communication component.	- ISA100 Wireless native protocol - Object mapping, tunnelling protocol - Extendable to support foreign protocols
Presentation	Establishes a context between application layer entities.	
Session	Controls the dialogues between computers. Establishes, manages, and terminates the connections between the local and the remote application.	- AES 128 bit encryption - Join key, network ID, end-to-end security - Device provisioning (OTA, IR, cable)
Transport	Reliable transmission of data between points on a network, including segmentation, acknowledgement and multiplexing	- UDP: Internet standard service - IPv6 addressing - Backbone routing
Network	Structuring and managing a multi-node network, including addressing, routing and traffic control.	
Data link	Provides the means for transferring data between two nodes connected by the physical layer. Detects and possibly corrects errors that may occur in the physical layer	- AES 128 bit encryption - Network configuration (mesh, star, hybrid) - Redundant communication to backbone (Duocast) - Channel hopping and blacklisting - Device roles
Physical	Transmission and reception of raw bit streams over a physical medium.	- IEEE 802.15.4 standard - 2.4 GHz ISM band

Table 1: Communication protocol stack with ISA100 Wireless implementation.

The system manager is a specialized function that governs the network, devices, and communications. The system manager establishes all communication relationships (contracts) for devices in the network. The contract between the system manager and a device in the network allocates network resources to support the particular communication need of this device.
A device with the backbone routing role acts as an open system interconnection between the wireless network and an internet protocol (IP) backbone. An ISA100 Wireless backbone router is commonly called an “access point”.
A device with the gateway role translates ISA100 Wireless messages to other formats such as Modbus. A gateway marks the transition between communications compliant to the ISA100 Wireless standard and other communications and acts as a protocol translator.

2.2.2 Different network topologies

ISA100 Wireless supports different network topologies. The simplest network topology is the star. In the star topology (see Fig.1) an access point communicates directly with each wireless field device. This topology will minimize the latency because each device is directly linked to an access point. With multiple access points, secondary (backup) links can be established.

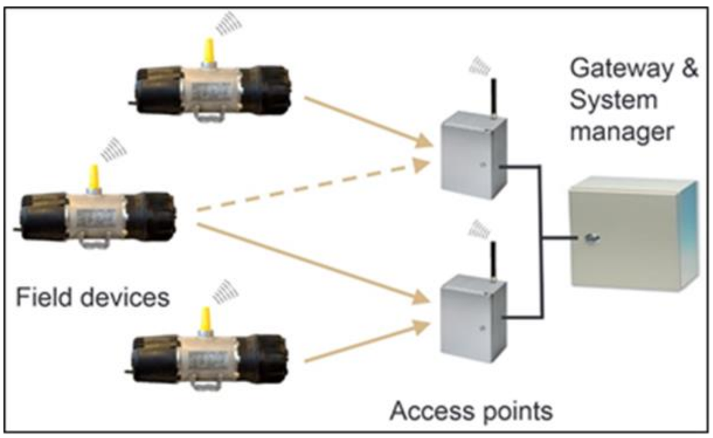

Figure1: Example of a star topology network with paired access points. Secondary (back-up) communication links are indicated with dashed arrow.

In a mesh topology (see Fig.2) all devices are capable of communicating with all other devices within radio range by assuming the routing function creating the topology shown in Fig.2. Wireless mesh topology is used to extend coverage by means of intermediate links and may enhance communication reliability by providing redundant paths between devices. Note that ISA100 Wireless supports the control of the maximum number of intermediate radio links (also named hops) from a field device to the access point. This is important to guarantee latency in a mesh topology network. ISA100 also allows the possibility to have a combination of a star and mesh topology known as a star-mesh.

2.3 ISA 100 WIRELESS STRENGTHS

2.3.1 Protocol support

One of the great strengths of the object-based ISA100 Wireless standard is the support of foreign protocols in the application layer (See Table 1) This universal application layer enables communication to any host system protocol such as HART, PROFIBUS, Foundation Fieldbus and many more. Vendors can build products to support various protocols while end users only need to deploy one single wireless network. Moreover, safety applications that need to comply with the functional safety standard IEC 61508 are also possible in an ISA100 Wireless environment. The open safety protocol PROFIsafe is SIL3 certified and when added to the ISA100 Wireless application layer then safe end-to-end communication between field devices and the safety controller is possible.

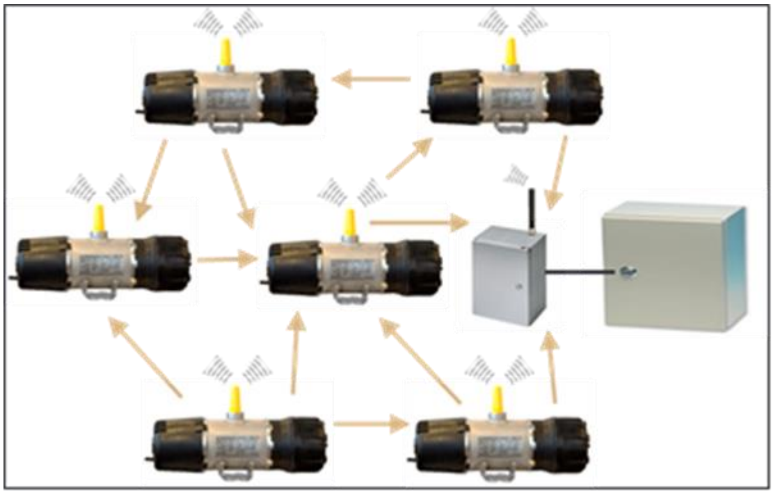

Figure 2: Example of a mesh topology network. All field devices operate as routers.

Note that WirelessHART is a command-based protocol confined to using HART commands for message exchange. Therefore, foreign protocol support is missing and safety (SIL) applications cannot currently be implemented in a Wireless HART environment.

2.3.2 Security

ISA100 Wireless provides robust, multi-tiered, policy-based security to ensure the safety of system operations. Communications are protected using a time-enhanced application of the 128-bit Advanced Encryption Standard (AES). Only devices that have legitimate and unique secret join keys are admitted to the network. Multiple-tiered AES-128 keys are derived from join keys and updated periodically. This secure key derivation method is the basis for a trusted relationship that makes the ISA100 Wireless network secure throughout the entire system life cycle. As shown in Table 1; ISA100 Wireless security operates at two levels in the Session layer and the Data Link layer. This means that both the transmitted data and the network are protected by advanced encryption.

2.3.3. Interoperability / Coexistence

Since ISA100 Wireless operates in the popular 2.4 GHz band it may be subject to interference from other wireless networks operating in the same frequency band (for example WiFi communication according to the IEEE 802.11 standard). Refer to Fig. 3 for an illustration.
To mitigate the effects of interference wireless protocols may employ various coexistence mechanisms. Clear Channel Assessment (CCA) and channel blacklisting are the preferred mechanisms to mitigate the negative influence from other proximal wireless networks. CCA is used to determine the current state of use of a wireless medium and aids in contention avoidance. CCA is best described as a "listen-before-talk" algorithm.
ISA100 Wireless also supports the simpler manual channel blacklisting where a network operator will manually configure which channels are available and which channels are blocked plus a more advanced adaptive blacklisting

mechanism; where each device in a network may autonomously blacklist channels which suffer from excessive noise and/or direct interference. Furthermore ISA100 Wireless supports four different CCA modes. In contrast Wireless HART currently only supports manual channel blacklisting and one CCA mode, only.
Therefore, ISA100 Wireless is best equipped to handle coexistence with other (e.g. Wifi) networks operating in the same frequency band.

between two devices in a network. A contract is an agreement between the system manger and a field device that involves the allocation of network resources by the system manager to support the communication requirements of the device and guarantee the limits for bandwidth, latency, and priority. This is an essential feature for safety applications making sure that messages from safety field devices are transported through the network within guaranteed time limits under all circumstances.

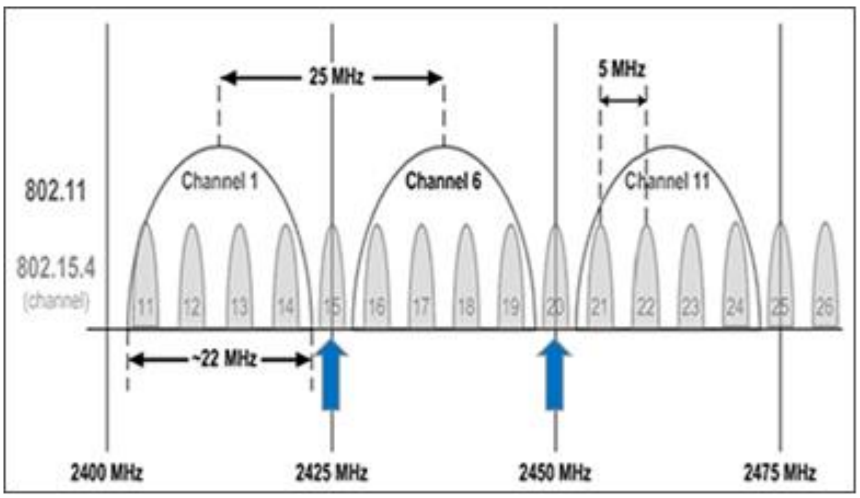

Figure 3: Illustration of the frequency spectrum covered by WiFi channels and ISA100 channels.
Note that ISA100 channels 15 and 20 are always free from WiFi interference.

2.3.4. Quality of service

Quality of Service (QoS) is a measure of the service quality that a network offers to applications and/or users. With QoS comes the ability to control the resource sharing of a network by giving different priorities to various applications and data packets depending on their requirements. Higher performance levels can be provided to specific applications and data packets through a set of measureable service parameters such as latency, packet loss, priority, and availability.
ISA100 Wireless uses contracts to define the setup and requirement of communication

In contrast, Wireless HART offers only one priority level for process data, meaning that all field devices in a wireless network share the same priority level and messages are delivered with a time delay as restricted by the bandwidth available at the time.

3.0 HOW TO ACHEVE SAFE WIRELESS

Achieving safe wireless is exemplified by the GasSecure GS01 gas detector. This is a battery powered field device specifically designed for wireless safety and monitoring. The GS01 fully supports the ISA100 Wireless standard and is therefore very easy to deploy in an ISA100

environment with compliant gateways and other ISA100 field devices.
The GS01 gas detector is also fully compliant with the SIL (Safety Integrity Level) guidelines as described in the IEC 61508 standard. This notably includes communications with a safety controller, which demands that all network traffic must be fully controlled and loss of contact to any field wireless device must be identified immediately.

3.1 REQUIREMENTS FOR SAFE WIRELESS COMMUNICATIONS

For industrial safety-related applications, continuous monitoring is required and a short response time (also referred to as latency) must be guaranteed when a safety critical situation occurs. For gas detection the average bandwidth requirement for wireless communication is fortunately modest. The primary challenge in designing a wireless safety system is combining a guaranteed short latency with very low power consumption. GasSecure developed the SafeWireless© communication concept to answer this challenge. In addition to combining low power operation with a short response time, the SafeWireless© concept also guarantees full control of all network traffic and immediately identifies any loss of contact with a field device.
Safe communication is based on cyclic exchange of messages *ie*. all data packets need to be answered one-by-one. All communication is initiated by the safety controller, which will send a data packet that must be answered by the field instrument within a process safety time limit. For hydrocarbon gas detection, this process safety time is defined by the IEC 60079-29-1 standard as 60 seconds. Once the controller has received a response from the field device it will immediately issue the next data packet. If the field device does not respond before the process safety time has elapsed then this device is marked as unavailable in the control system.
For wireless data transfer it is advisable to allow several attempts for transmitting a data packet within the process safety time in order to achieve robust and reliable communication. For the GS01 a reasonable balance between low energy consumption and robust wireless communication is to have three to five attempts within the process safety time; *ie*. one downlink data transmission every 12 to 20 seconds.
The GS01 device is specified as having a 5 sec. (T90%) response time. In order to fulfil this response time specification there need to be defined timeslots every two seconds for uplink data packets. The GS01 gas detector during initial configuration will therefore request that sufficient bandwidth be set aside for this uplink transmission rate. In the absence of detected gas not all of these frequent timeslots will be used and the GS01 will limit communication to once every 12 to 20 seconds thereby minimizing the average power consumption.
In the presence of hydrocarbon gas the GS01 needs to report the detected gas concentration immediately and with the earlier stated 5 sec response time. However, downlink data packets arrive only every 12 - 20 seconds and there is a one-to-one mapping between incoming packets and the device response to them. In other words, once the detector has responded to a data packet it is unable to report gas concentration until the next data packet is received from the safety controller. This apparent dilemma is solved in SafeWireless© by holding the response to a data packet until just before the following data packet is expected. This way the "blind" time is minimized to the two second contract period and the detector is always primed and ready to report gas immediately.
This concept; with two modes of communication for “No Gas” and “Gas”, as illustrated in Figs. 4 and 5, is unique to the GasSecure GS01.
The SafeWireless© communication also fulfils the requirements of functional safety standard IEC 61508 for Safety Integrity Level (SIL) 2 capability. Most importantly the following four error-handling mechanisms are supported: sequence numbering, timeout in the absence of response, device code name and data consistency

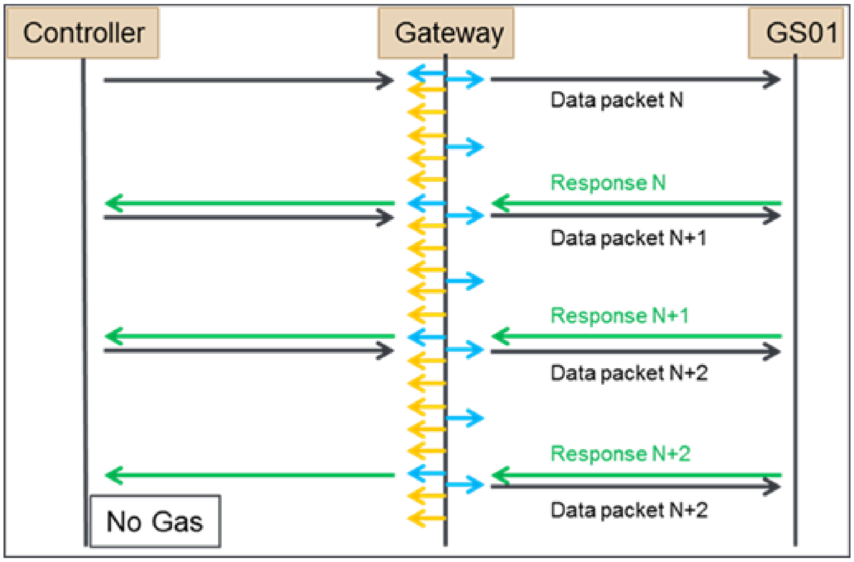

Figure 4: SafeWireless© communication in the absence of hydrocarbon gas. The GS01 is set up to only use every 6th of the 2 sec uplink communication slots allowing for transfer of 5 data packets per minute. Yellow and blue arrows indicate allocated timeslots for uplink and downlink communication, respectively.

checking. The purpose of these mechanisms are to detect failures of the safety device in terms of *eg*. packet loss, unacceptable network delay, bit errors, and replay attacks.

Several options exist for implementing these required safety features. The approach chosen by GasSecure is to utilize a certified implementation of an open safety application protocol. Due to its widespread use in safety and process control applications GasSecure has identified PROFIsafe over PROFINET as being a suitable protocol.

As stated earlier PROFIsafe is added to the application layer of the ISA100 Wireless communication stack (cf. Table 1). PROFIsafe is one of the few non-proprietary SIL-certified tools for safety communication loops and fully supports the aforementioned error-handling mechanisms. In a wireless gas detection system, PROFIsafe covers the entire communication path from the field device to the safety controller (end-to-end communication). PROFIsafe signals are only visible to the field device and the controller. Because of this so-called “Black-Channel” principle, the PROFIsafe layer (located above the standard protocol) has no impact on the standard bus protocols and is independent from the base transmission channels. Therefore, gateways do not require SIL certification not even when part of SIL certified communication loops.

3.2 CONCLUSION

ISA 100.11a has the capability needed to be the wireless sensor network of choice to handle safety related communication, proven by third party end to end SIL2 certification by Exida.

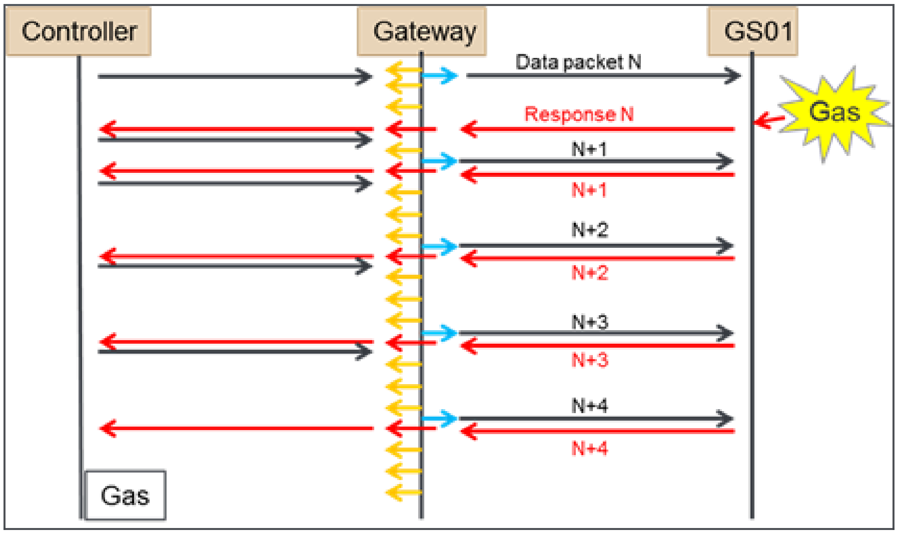

Figure 5: SafeWireless© communication in the presence of hydrocarbon gas. On the occurrence of gas the instrument responds instantaneously (red arrow) using the first available timeslot (yellow arrow) for uplink communication. Communication is more frequent in the presence of gas i.e. all timeslots for downlink communication (blue arrows) are now used.

4.0 FUTURE DEVELOPMENTS FOR SAFE WIRELESS

Due to the latency capacity of ISA100 and the quality of service, this wireless protocol operates with response times of seconds rather than hours and minutes. This capability is influencing the market to provide more safety related devices. Today there are a handful of devices aimed at safety. These include gas detection, safety shower activation, sprinkler activation and similar inputs. Over the coming years an increasing number of devices are expected to come to market with 3rd party verification of a SIL loop from device to system. This has been achieved with ISA100 and tunneling even if the protocol was not initially intended to be used for this automated safety action:

4.1 Open protocol decreases time to market

The advantage of an open protocol and clear Guidelines of the Wireless Compliance Institute (WCI) the time-to-market for devices is significantly reduced. Referring to Fig. 7 the adaptation of wireless in safety is moving from the mainstream adoption into satisfying the highest performance standards for instrumentation.

4.2 Devices of tomorrow

The range of input and output safety devices to be realized in the near future gives any user with an existing wireless infrastructure a vast advantage over those that have not made the transition. ISA100 members will be able to collectively supply total safety packages for customers including full fire and gas detection, audible and visual alarm indicators, heat sensing cable, leak detectors, alarm pushbuttons, *etc*. The initial driver for wireless use was the attraction of project cost reductions where up to 90% of installed cost of conventional measurement technology can be for cable conduit and related construction. Wireless infrastructure can reduce the typical installation time with 80% and cost by 50-80% depending on the scalability of the system. Wireless also has the ability to add safety by being flexible and reduces the cost of changes to adapt to new safety challenges.

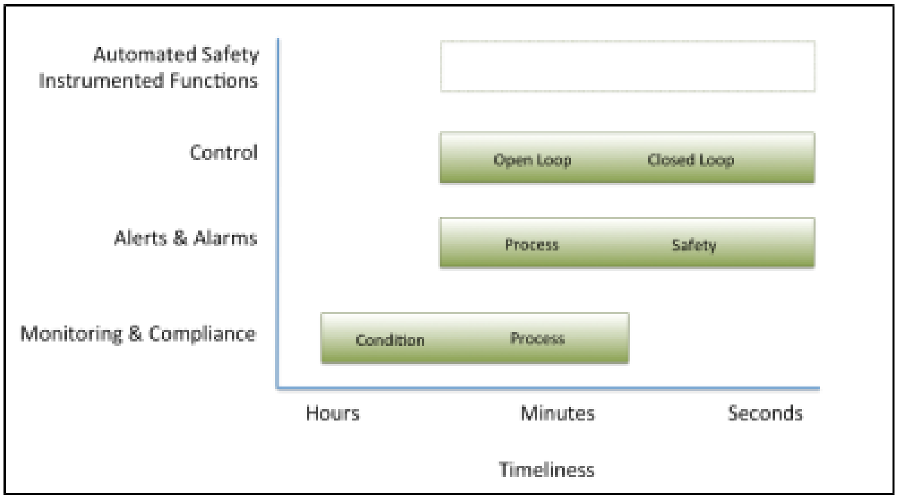

Figure 6. Service time requirements depending on application. (AIW LLC)

5.0 GUARANTEEING WIRELESS INTEROPERABILITY

An important aspect for end users regarding ISA100 devices is that the WCI conducts interoperability events. Interoperability events are an important dimension of the WCI's technical program and provide WCI member organizations an opportunity to validate the interoperability of devices.

Interoperability events provide realistic tests and permits WCI quality assurance processes to ensure that functional tests conducted during ISA100 Wireless certifications provide proper coverage for the ISA100 Wireless Implementation Specification. This process gives confidence that ISA100 devices from any WCI member will interoperate in any validated system supplier's network.

These events provide ongoing validation of the ISA100 Wireless certifications, identify areas for new test coverage as new categories of devices are added to the ISA100 Wireless portfolio, and provide input for improving the usability of the ISA100 Wireless certification test platform. The interoperability tests also bring together the different suppliers as a technical community building relations over technology to achieve a common goal. This creates a discussion platform around the use of technologies and a forum for how they can be combined to give customers added value.

As a result end users can therefore select ISA100 Wireless Compliant™ devices from a best-of-breed pool of suppliers with assurances of device interoperability.

ISA100 Wireless (IEC 62734) is an international, industrial wireless networking and communications standard engineered to support the next generation of Industrial Internet of Things (IIOT) technology and includes support for the needs of process industries. With native IPv6 networking and object architecture, ISA100 Wireless extends the IIOT to wireless.

ISA100 Wireless enables automation engineers to quickly create, modify, optimize, and scale wireless networks that are open, interoperable, and reliable for their most critical applications

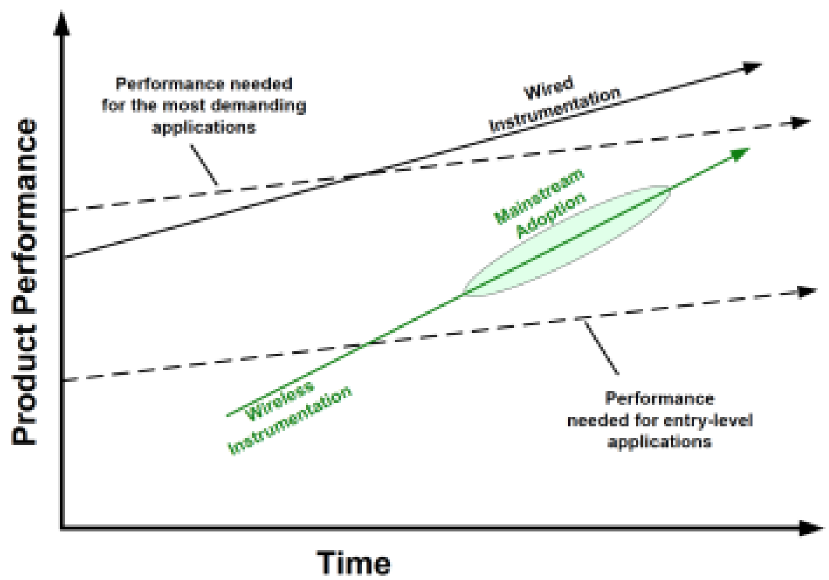

Figure 7: Christensen innovation model adapted for industrial wireless.

6.0 ISA100 PROVEN IN USE

At the time of writing ISA100 has over a billion hours of operating time and is used in a variety applications:

- Machine health monitoring
- Basic process control
- Monitoring of well heads
- Remote process monitoring
- Leak detection monitoring
- Diagnosis of field devices
- Condition monitoring of equipment
- Environmental monitoring
- Tank level monitoring
- Gas detection
- Fuel tank gauging
- Steam trap monitoring
- Open loop control
- Stranded data capture

This is why it is important for end users to look at their total needs for enhanced coverage by wireless. Large savings are realized when the total solution capabilities of all suppliers is leveraged.

6.1 CASE 1: REDUCTION OF COST WITH INCREASED SAFETY AND FLEXIBILITY

A large European oil and gas company decided to roll out a complete site wide wireless network in their main gas processing plant. The rationale for doing this was cost savings, increased flexibility and speed of response to local challenges.
The site has been in operation for more than 20 years and has been through several minor and major modifications over the decades. Pipes and process equipment have been exposed to fluids and gases, slowly wearing the installation down. At this stage, the site has now realised that they will need to monitor the wear and tear more carefully and want to install temperature, vibration, corrosion and gas detection instruments. By implementing a wireless network covering the whole site they are able to cost effectively implement required added

instrumentation, on short notice, without involving too many technical disciplines. Planning, engineering and installation of equipment to support wired instruments takes time and can potentially increase risk of day to day operation as installation work can interfere with existing infrastructure. Wireless can however be installed in parallel without any required physical modifications on junction boxes, cable trays or trenches.

6.2 CASE 2: ACHIEVING SIL2

The Statoil, Kalundborg refinery, in Denmark is a 35-year-old installation. Due to lack of documentation regarding what they could find in the ground when digging and the high cost of building structures above the ground, they decided some years ago that wireless could be of great benefit to them. The refinery has been using ISA100 wireless for more than 5 years on temperature and pressure transmitters. When the requirement came up to increase their gas detection on site they were happy to have a look at wireless also for this. The requirement was for SIL2 certified detectors and GasSecure was the only company who could support this and wireless at the same time. The refinery initially installed 122 wireless gas detectors in their process area in 2016. Since then they have increased the number of gas detectors simply by adding sensors to the already installed network. These additions have been done at little more than the cost of the units. Based on the positive experience with wireless the site staff are now potential extensions to cover other areas with additional devices.

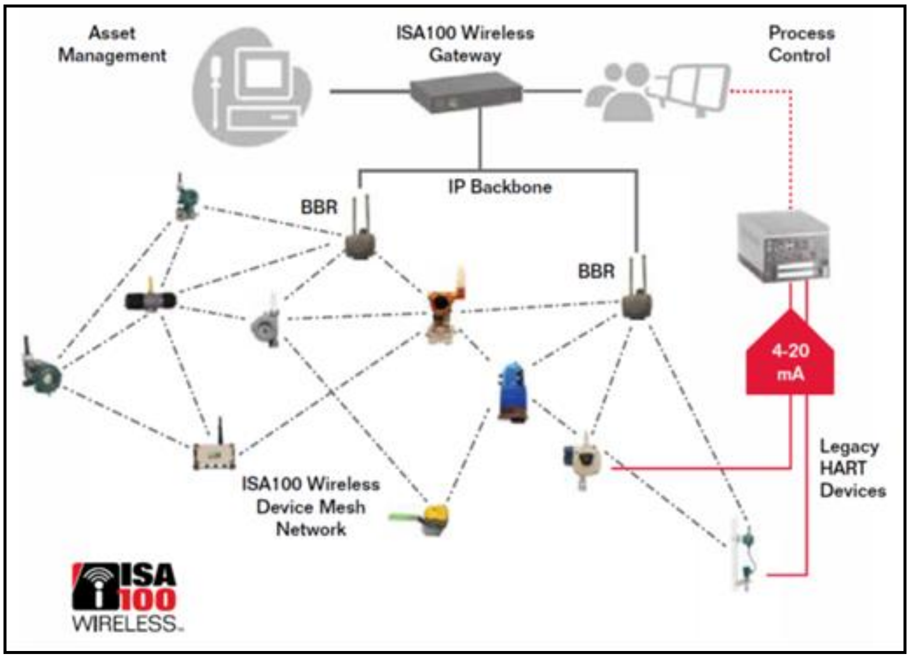

Figure 8: ISA100 wireless interoperability.

Figure 9: Location and types of interoperability applications of ISA100 devices.

7.0 CONCLUSION

Wireless for safety applications has been available since 2012. The technology has caught up with customer needs, and documenting the safety from device to control system is also achieved. Looking at the cost focus in the current market the drive for more cost efficient solutions, the potential for every single one of the wireless devices in a sensor network gives end users a strong benefit both in economical and flexibility terms. Traditional thinking is that wired is the safest way one can connect, this needs to be challenged. Is a system still hardwired if you convert it to light and use a fibre cable? If an accident happens at site, will a cabled system selfheal and find its way back together like a wireless system? After an incident, if multiple cables are destroyed, how fast will you recover compared to a wireless system? After looking at process safety related information, design of devices and control systems the time is now for utilizing the possibilities of wireless. To make the most of a wireless installation, end users need to get information on available devices in the market. Another good source of information is to look at the vast number of application notes that are available describing success stories across the industry. Finally, it is important to talk to suppliers of equipment to get a sense of which products are coming to market. For suppliers, input from end users is essential, the entire ISA100 and all devices available start with a market demand. If you have challenges in your operation these can be changed into solutions based on cooperation and development.