Evolution of Wireless Sensor Networks for Industrial Control

Arthur Low

> *"The history of life is more adequately represented by a picture of 'punctuated equilibria' than by the notion of phyletic gradualism. The history of evolution is not one of stately unfolding, but a story of homeostatic equilibria, disturbed only 'rarely' (i.e., rather often in the fullness of time) by rapid and episodic events of speciation."*
>
> Niles Eldredge and Stephen Jay Gould
> (1972; tinyurl.com/ak34qt3)

Technologies evolve in a process of gradual scientific change, but the commercial application of technologies is discontinuous. Managers interested in technology evolution can integrate these contrasting ideas using a powerful theoretical framework, based on the concept of punctuated equilibrium from evolutionary biology. The framework, which enables the differentiation of the technical evolution of a technology from its market application, is used in this article to compare the two standards for wireless sensor networks (WSN) for industrial instrumentation and control: WirelessHART and ISA100.11a.

The two WSN standards are the product of two different market contexts, which have selected different minimum viable technologies for evolution in their respective niches. Network security issues present some important selection criteria. Both WSN standards implement security countermeasures against localized wireless network attacks based on the application of the AES encryption standard, but some specific security threats – some local, others remotely launched – are only well-defended by the adoption of public-key cryptographic (PKC) protocols, which only ISA100.11a supports. This article concludes that the mainstream market potential of the Internet has influenced the evolution of ISA100.11a and will continue to demand that each WSN standard evolve in ways that are difficult to predict.

Introduction

Comparisons between the two standards for wireless sensor networks (WSN) for industrial instrumentation and control commonly view WirelessHART (WH; tinyurl.com/bblesph) and ISA100.11a (ISA; tinyurl.com/bba9gdp) as competing standards, and they tend to conclude that one standard is better than the other. Consider the titles of recent comparisons in two widely read industry trade journals: "WirelessHART Wins Standards Battle Against ISA100.11a" (*Control Design*, 2012; tinyurl.com/a35d3tw) and "ISA100.11a Completely Obviates the Need for WirelessHART" (*Petro Industry News*, 2007; tinyurl.com/a9ddkty). However, such comparisons are more likely confuse than educate the industry. The former article described "standards confusion" and fading hope within the industry for a convergence between WirelessHART and ISA100.11a. The goal of this article is to help relieve some of this apparent confusion in the control industry that may be the consequence of previous, "winner-take-all" technically-driven comparisons of the two WSN standards.

This article compares the two competing WSN standards for industrial control, not based on purely technical dimensions, but based on a theoretical framework of technology evolution, drawn from the technology innovation management literature. Thus, this article is a tangible application of theories and approaches to technology innovation. The theoretical framework enables the gradual evolution of WSN technology to be differentiated from its discontinuous commercialization in the automation and controls industries.

The article is structured as follows. First, the theoretical framework is introduced and its methodology is explained by referring to the development of wireless technology in the 19th and 20th centuries. Next, the two WSN standards – WirelessHART and ISA100.11a – are compared. The framework is then applied to differentiate each technology from its market application. Next, two market contexts are presented based on the networking and security differences of the two standards. Finally, conclusions are provided.

Theory of Punctuated Equilibrium

The following two perspectives on technological change appear to be inconsistent, and therefore hard to reconcile without a suitable theoretical framework: i) technology undergoes gradual and incremental scientific progress, and ii) the commercialization of the technology is both rapid and discontinuous. The theory of punctuated equilibrium, derived from evolutionary biology, offers a powerful theoretical framework (Adner and Levinthal, 2002; tinyurl.com/a5t62bx) to reconcile apparent inconsistency between the gradual change in underlying science and the discontinuous commercial applications of technologies. The theory was introduced to explain the inconsistency between the fossil record and Darwin's concept of gradualism. The inconsistency was resolved by noting that speciation events allowed the separate evolution of one population from its antecedent. Two critical features of speciation were observed. First, speciation is genetically conservative; it does not follow from a sudden genetic transformation of the population. Second, the distinctive growth of the new species following the speciation event is the result of the different selection environments.

The theoretical framework of punctuated equilibrium defines a method to identify the critical transition point when emerging technologies realize commercial importance. The analogue of a speciation event in technology is the application of existing technologies to a new domain. After the speciation event, major commercial impact may be observed if there are available resources and selection processes that drive rapid technological development to adapt to the environment featured in the new domain.

Framing technology evolution in terms of a speciation event allows a technology's technical development and its market application to be differentiated. This allows a manager responsible for a technology innovation to make better plans for R&D activity to match the needs for innovation and the available resources of a real market. Changes in an application's domain signal significant shifts that define different selection criteria concerning a technology's minimum viable functionality, such as an emphasis on specific critical functionality from the general prototype function and available resources to drive innovation.

Radically divergent technology and rapid technological change can follow a speciation event. The framework of punctuated equilibrium specifies that the nature and pace of technological change are driven by two elements of the selection process. First, the process of adaption begins when the prototype technology (with a minimum threshold viability) becomes adapted to the particular needs of the new niche. Second, resource abundance within the niche drives the pace of development, especially if the applicability of the technology in terms of more functionality or lower cost can extend to more mainstream markets.

When technology that emerges from its speciation event is ultimately able to successfully invade other niches, possibly including the original domain of application, creative destruction can occur, meaning that a new combination of technical and business-model innovation destroys the incumbent's capital.

Framing the evolution of wireless technology
The development of wireless technology offers an example of how the theoretical framework of punctuated equilibrium can be applied to the evolution of WSN technology for automation and industrial control.

Table 1 shows how the theory of punctuated equilibrium applies to the development of wireless communications in the late 19th and 20th centuries. Hertz developed wireless instruments to prove Maxwell's theories of electromagnetic (EM) waves, then Marconi selected Hertz's minimum viable EM equipment for the sending and receiving of radio wave signals over long distances. This was the speciation event.

Evolution of Wireless Sensor Networks for Industrial Control

Arthur Low

Table 1. Evolution of wireless technology

Technology	Domain	Selection	Resources	Outcome
EM Pulse	Science	Prove theory	Low	Instrument
	Commerce	Ship-to-shore communication	High	Vacuum tube
Vacuum Tube	Niches	Police radio	Moderate	Private radio
	Mainstream	High quality & low cost	Massive	Broadcast radio & TV

Abundant resources were applied to the niche for ship-to-shore communications. Transmitter power and receiver sensitivity were selected for improvements, which led to the development of the vacuum tube and the analog-electronics industry. Primitive tubes that enabled transmission and reception of low-quality audio (i.e, sufficient for understandable speech) were immediately selected for mobile radios for police and military applications. Over time, comparatively modest resources offered by the niche markets improved the audio quality. Eventually, massive resources were allocated by large corporations to develop and mass-market radio and TV broadcast technology.

Comparing WH and ISA

The Institute of Electrical and Electronics Engineers (IEEE; ieee.org) standard for low-rate wireless personal area networks (LR-PAN) is 802.15.4 (tinyurl.com/a3tdv54), which specifies the first two layers in the Open Systems Interconnection (OSI) model: the physical (PL) layer and the media access control (MAC), or data link, layer.

The PL operates with carrier sense multiple access with collision avoidance (CSMA/CA). WH and ISA use the 2.4 GHz band with 16 channels. The MAC layer specifies the frame with header, payload, and check fields for the reliability and integrity of the frame. The latest version of the MAC layer standard, 802.15.4-2006 (approved by the IEEE in 2012), adopts the ISA100.11a standard for network synchronization using time division multiple access (TDMA) with 10–14 mS variable time slots and three channel-hopping schemes.

Figure 1 shows that PAN networks can take on both star and peer-to-peer configurations, including full-function devices (FFD) and reduced-function devices (RFD).

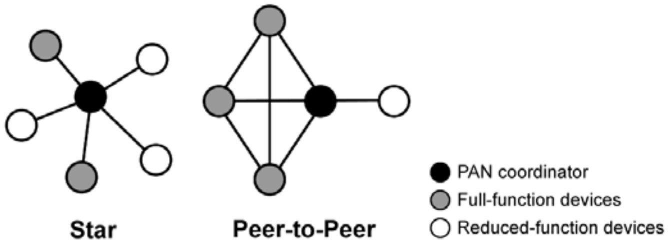


Figure 1. PAN network topology
(Adapted from: tinyurl.com/a3tdv54)

The network (star or peer-to-peer) is controlled by the PAN coordinator. Peer-to-peer networks enable “ad hoc” formation of a more complex network called a “mesh”. Mesh routing is a network (OSI layer 3) function, which is not specified by IEEE 802.15.4. Nevertheless, in the peer-to-peer network shown above, there are several routes from the PAN controller to the FFD node to its left. The distance from one node to another is measured in “hops”.

WH specifies a number of device types in its network, specifically gateway (G), security manager (S), network manager (M), access point (AP), field device (F) and a hand-held provisioning device (PD). ISA specifies system manager (M), security manager (S), gateway (G), backbone router (B), router (R), input/output node (IO), routing IO node, and a portable (P) device. These devices and their general connection diagrams are shown in Figure 2.

Redundancy is an important design consideration for critical industrial-control applications. Both networks show redundancy. In the WH network, G can connect to any F through either AP. In the bottom ISA network, redundancy is shown such that the GMS can connect to

Evolution of Wireless Sensor Networks for Industrial Control

Arthur Low

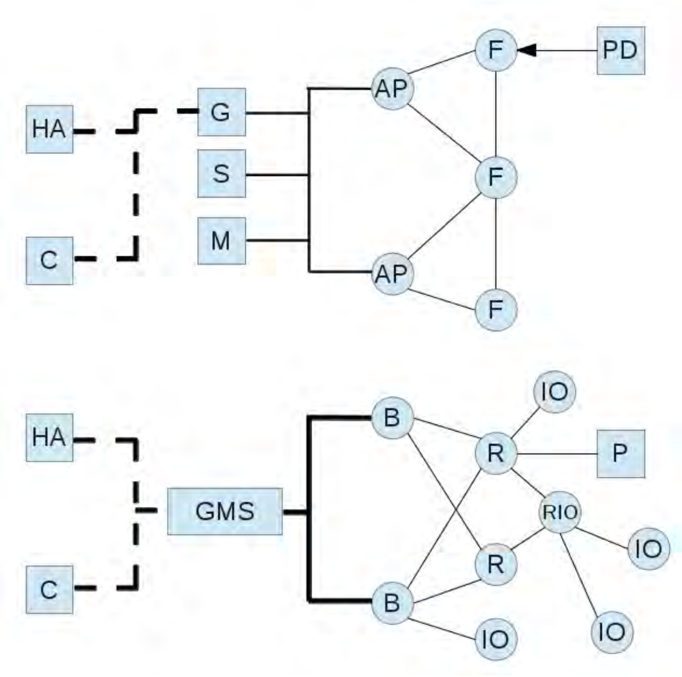


Figure 2. General network architectures: WH (top) and ISA

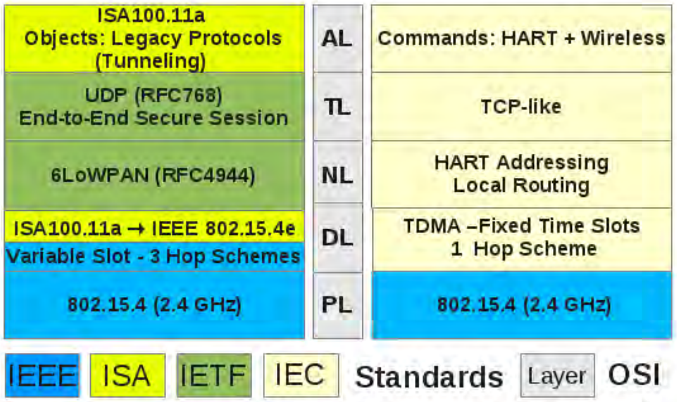
the RIO through any B and R node. The ISA network also shows a backbone network (solid thick line) connecting the GMS and the backbone routers.

In Figure 3, the OSI model is used in this article to compare the two WSN standards. The ISA100 Wireless Compliance Institute's depiction of its OSI stack (left) is shown beside the WH OSI stack (right). The layer abbreviations are shown between the ISA and WH stacks. Note that the ISA stack is based on several Internet Engineering Task Force (IETF; ietf.org) requests for comments (RFC) and the standards from IEEE and ISA.

Similarities and differences

Beginning at the physical layer (PL), both standards use IEEE 802.15.4 radios operating at 2.4 GHz, and at least passive neighbour discovery, channel hopping, and TDMA time-slots at the data link layer (DL).

The differences begin at the DL. WH supports a fixed 10 ms time-slot and just one channel-hopping scheme. ISA specifies 10–14 ms variable time slots, three channel-hopping schemes, and active neighbour discovery. The ISA network layer (NL) supports IPv6 addressing by adopting the IETF Internet Protocol version 6 (IPv6) over low-rate personal area networks (6LoWPAN) standard. Sub-net routing is also supported, whereas WH supports local routing based on HART addressing.



ISA100.11a Objects: Legacy Protocols (Tunneling)	AL	Commands: HART + Wireless
UDP (RFC768) End-to-End Secure Session	TL	TCP-like
6LoWPAN (RFC4944)	NL	HART Addressing Local Routing
ISA100.11a → IEEE 802.15.4e Variable Slot - 3 Hop Schemes	DL	TDMA –Fixed Time Slots 1 Hop Scheme
802.15.4 (2.4 GHz)	PL	802.15.4 (2.4 GHz)

Figure 3. WH and ISA mapped to OSI layers

At the transport layer (TL), ISA is 6LoWPAN-compatible, based on UDP, whereas WH specifies a TCP-like (connection-oriented, reliable) data-transport mechanism. Both standards aim at efficiency of message passing between applications. The WH application layer (AL) is command-oriented (commands were added to HART commands to support wireless operation). WH commands can be aggregated. ISA is object-oriented at the AL. Object-based messages can be concatenated.

ISA supports 6LoWPAN

6LoWPAN enables the transport of IPv6 packets over IEEE 802.15.4 low-rate wireless personal area networks (LoWPANs). IEEE 802.15.4 frames are too small for the maximum size of an IPv6 packet. To support 6LoWPAN, between the NL and DL, header encapsulation, compression and fragmentation mechanisms were defined. As a result of 6LoWPAN compatibility at the NL and DL, ISA supports the development of backbone routers.

Security considerations

Both standards provide two layers of network security. The DL applies a message integrity check (MIC) in WH, whereas ISA supports several MIC or encryption security policies inherited from the IEEE 802.15.4 MAC layer. Based on these policies, ISA can selectively encrypt and authenticate the MAC payload. The use of several types of symmetric keys is presenting in Table 2.

A join key is defined in both standards to be used by the device to join the target network using an authorized password. The join key acts as a session key between the node and the network manager during the join process. In WH, the symmetric join key is transmitted to the node when the device is provisioned. ISA supports

Table 2. WH and ISA key-management schemes

Key	WH	ISA	Function
Join	Encrypts	Authenticates	Enables node to join the network
Data Link	DL Key MIC (all nodes)	NL Key MIC / Encrypt (sub-net)	Written to node by security manager (SM)
	Join Key	Master Key	SM encrypts with the join key
Session	Network	Transport	Written to node by security manager (SM)
	Join Key	Master Key	SM encrypts with the join key
Global	Well-known	K_Global	Used to authenticate during join process
Master	N/A	Never transmitted	Generated by node and SM using PKC and provisioned credentials

symmetric and asymmetric keys. Using asymmetric keys, the symmetric keys used by the node can be regenerated without repeating the device-provisioning process.

A DL key is used by WH, whereas an NL key is used by ISA. The purpose is the same: to provide encryption between devices as the message “hops” along the network. But, the DL key is the same for all WH devices, because messages may traverse the entire network, whereas more specific sub-network keys can be defined in ISA.

Both WH and ISA support end-to-end security. A session layer (SL) key (session key) enables secure transfer between end points, at the TL for ISA and the NL for WH. ISA supports peer-peer secure sessions, say between a gateway and network device.

Key distribution and provisioning
A hand-held device is plugged into the WH node to provision it using only symmetric keys. The join key is written to the WH device to provision it for the specific network. The network manager can then write the NL key and the SL key (encrypted with the join key) to the new device after it joins the network.

ISA supports dynamic key distribution using asymmetric keys based on the principles of public-key cryptography (PKC). PKC enables over-the-air (OTA) provisioning, as well as automated “re-keying”. The security credentials for each node are provisioned. Then, all keys are derived from the asymmetric master key (private key) that is generated inside each device using a secure key generation (SKG) process. Asymmetric SKG enables both devices to create a shared secret master key without ever transmitting the master key between nodes. The DL key and SL keys are then encrypted with the master key and written to the node.

WSN-based security threats
WH and ISA inherit threats common to all IEEE 802.15.4 WSN installations (Alcarez and Lopez, 2010; tinyurl.com/azkdux4). Generally, these threats can be mitigated by the installation of an intrusion detection system and by adopting the recommended countermeasures.

WH has two vulnerabilities that ISA avoids due to adoption of a PKC-based key-management scheme (PKC-KMS) as part of its suite of recommended countermeasures for IEEE 802.15.4 LR-WPANs. Although rarely applicable, WH is vulnerable to the Sybil attack (tinyurl.com/65mygp) if the security policy of the network does not specify the frequent updating of the NL and SL keys. WH is vulnerable to a sniffing attack, depending on the rate of provisioning of new nodes, which affects how fast the WH network can update its security credentials. ISA avoids sniffing attacks by using time-limited network and session keys. ISA prevents a Sybil attack by a strong challenge-response process that ensures the security manager issues unique contracts to all nodes, and by the periodic updating of all security credentials.

Framing the Evolution of WH and ISA

The framework of punctuated equilibrium defines a speciation event as the application of existing technology to a new domain. Using this theoretical framework, we start by considering what existing minimum viable technology was available for selection as an outcome of the evolution of electronics and computers.

The growth in complexity of computer programs led to the development of object-oriented software libraries. Open source development communities expanded on the proprietary technology-driven business models and have been major contributors to the development of the Internet. The Internet Protocol (IP) has expanded to IPv6 to enable uncountable numbers of interconnected devices. IPv6 has been further extended to low-rate personal area networks to produce 6LoWPAN, which essentially merges wireless mesh networks with the Internet backbone. Advances in symmetric and asymmetric cryptography and hashing algorithms have enabled robust end-to-end security to be applied effectively above the network layer and to the data link layer. Low-power wireless semiconductors and embedded software systems on chips enable self-organizing machine-to-machine mesh networks.

Table 3 shows the evolution of the base technologies that are the ancestors of WH and ISA. For example, starting in the left column, the general technology domain of electronics and computers was migrated to three new sub-domains: software, security and wired controls. In the case of the software sub-domain, the growth of software-program size led to increased software complexity that caused problems with maintainability, reusability, and reliability. Efforts to handle software complexity were therefore highly funded, and the outcome was the innovation of object orientation. The technology evolu-

Table 3. Evolution of WSN automation technology

Technology	Domain	Selection	Resources	Outcome
Electronics and computers	Software	Complexity	High	Objects Open source
	Security	Secure key generate	High	PKC
		Encrypt & authenticate	High	AES
	Wired controls	Industrial control	High	Sensors: HART + other standards
Internet	Machine to machine	Addressing	High	IPv6
Semi-conductors	Wireless	Low power Spread spectrum	High	IEEE 802.15.4
802.15.4 IPv6	LoWPAN	Low power reliable & IOT	High	6LoWPAN
Sensors 802.15.4 6LoWPAN Objects AES PKC HART + other standards	Wireless controls	HART Security	High	WH
	Wireless controls Internet	Industry standards Objects Security IPv6 LoWPAN OTA Provision	High	ISA

tion within the sub-domains of security and wired controls can be explained in the same way. The next two parent technology associations are for the Internet and semiconductors. The outcomes of these technologies were two new sub-species: Ipv6 network addressing and IEEE 802.15.4 low-power wireless personal area networking chips (LoWPAN). When these technologies mated, the offspring was 6LoWPAN. The last technology association is the cross-fertilization of a number of technologies that the framework identifies as the two speciation events that are the subjects of this article. WH was developed to adapt HART to the LoWPAN (wireless) domain. Resources were highly available and aligned to evolve WH. Multiple existing (and new) wired standards for industrial control and automation can directly use ISA to reach the LoWPAN domain.

Applying Market Contexts

Considering the difference between WH and ISA, there are two key market contexts that will drive innovation and channel resources that affect the pace and diversity of the evolutionary process unfolding:

1. **Heterogeneous Wireless Standards:** Heterogeneous wired-sensor installations can co-exist, but heterogeneous WSN standards based on IEEE 802.15.4 will compete and jam each other's spectra.

2. **The Internet:** The Internet is itself a rapidly evolving technology and applications ecosystem. The emergence of a WSN that can invade the Internet represents a mainstream opportunity.

Applying security considerations to these two market contexts, ISA offers defenses against sniffing and Sybil attacks, due to its PKC-KMS, which WH lacks. The implementation of a broad range of recommended countermeasures is essential for both types of WSN installations. Considering that 6LoWPAN is a parent technology of the ISA standard, clearly the ISA has enabled its standard to more easily adapt to the addressing requirements of the Internet with the WSN. Strong PKC-KMS is an important attribute of the ISA standard when considering Internet security.

Discussion

The framework of punctuated equilibrium requires recognition of a significant shift that defines different selection criteria for specific minimum viable functionality that must exist before it can be applied to the newly identified market niche. Industry has accepted WH, but the emphasis of the Internet as an application domain led to the selection of 6LoWPAN in ISA, which represents a major difference between the two WSN standards:

- WH extends the HART protocol to wireless by selecting the minimum viable functionality of IEEE 802.15.4-based WSN and symmetric-key algorithms for security.

- ISA extends the selection criteria of WH to include object orientation, 6LoWPAN compatibility, and asymmetrical cryptography.

Strong selection forces have created a speciation event for both WH and ISA by applying existing technology to new market niches. Each niche has applied different resources and emphasized different aspects of the technology to improve. Within those niches, innovations to WH and ISA have occurred at different paces, driven by differences in resource abundance and market demand for technological change.

The ISA niche invaded the original IEEE 802.15.4 niche. The inclusion of ISA MAC layer channel-hopping schemes and variable time-slots in the updated IEEE 802.15.4-2006 standard for LR-WPAN radios can now be seen as an important and possibly disruptive evolutionary event.

Conclusion

In this article, the framework of punctuated equilibrium was applied using a tabular method to compare the two WSN standards for industrial control. The method differentiated the gradual, continuous evolution of one or more antecedent technologies from their discontinuous and sometimes rapid commercial application inside several new sub-domains. This differentiation is called speciation. Two speciation events were defined as the establishment of two new, commercially important market niches for WirelessHART and ISA100.11a. Actors within each WSN sub-domain will select features of the technology for further evolution within the niche, which implies that they will evolve distinctly at a pace set by the resources available in each niche market. Technology innovators can identify opportunities by successfully analyzing what minimum viable technology the niche has selected for refinement. One such opportunity is the need for improved security features based on PKC technologies.

This article can therefore make two specific conclusions about the evolution of the two WSN standards. First, ISA's support for IPv6 via 6LowPAN, more robust network security by application of PKC-KMS, and application-layer support for heterogeneous legacy wired standards is significant. The influence of the ISA standard on the IEEE 802.15.4-2006 standard, which the framework of punctuated equilibrium identifies as an invasion of the antecedent application domain, is strong confirmation of the robustness of ISA's new niche. Second, market forces will work to evolve adoption of WSN technology by these two considerations:

1. The likelihood that other legacy wired automation standards will follow the HART model by extending themselves to IEEE 802.15.4 or adopting the ISA standard.

2. The pace of development of each standard and the technological emphasis on improving minimum viable functionality by market selection processes in the WH and ISA niches.

Looking to the future, major resources will be applied to bring industrial plant intelligence into the mainstream of the Internet.

Acknowledgements

I would like to thank Professor Michael Weiss of Carleton University's Technology Innovation Management program for suggesting the use of the evolutionary framework for the comparison of the two standards. Also, I would like to thank Jayson Shiu of Suncor Energy for suggesting the comparison of the WirelessHART and ISA100.11a standards. A version of this article was presented at the ISA Calgary Show 2013 in Calgary, Canada, April 17–18, 2013.

About the Author

Arthur Low is the founder and Chief Executive Officer of Crack Semiconductor, a supplier of high-performance cryptographic silicon IP used in some of the most demanding security applications. Arthur has a number of patents in the field of hardware cryptography. He has worked for a number of IC startups as a Senior IC designer and Architect and gained much of his fundamental IC design experience with Bell-Northern Research in the early 1990s and with IBM Microelectronics in the late 1990s. Arthur has a BSc degree in Electrical Engineering from the University of Alberta and is completing his MSc degree in Technology Innovation Management in the Department of Systems and Computer Engineering at Carleton University.

Citation: Low, A. 2013. Evolution of Wireless Sensor Networks for Industrial Control. *Technology Innovation Management Review.* May 2013: 5–12.

(cc) BY

Keywords: technology evolution, punctuated equilibrium, wireless sensor networks, standards, WirelessHART, ISA100.11a, industrial control