Safe and Secure Wireless Networked Control Systems

James H. Taylor [†], Johan Åkerberg [‡], Hazem M. S. Ibrahim [†], Mikael Gidlund [‡]

[†] *Department of Electrical & Computer Engineering.*
University of New Brunswick
Fredericton, N.B. Canada
jim.taylor@ieee.org, hazem.saad@unb.ca

[‡] *ABB AB, Corporate Research, Sweden*
P.O. Box 883
Forskargränd 7, 721 78 Västerås, Sweden
johan.akerberg@se.abb.com, mikael.gidlund@se.abb.com

***Abstract*— Wireless technology has gained much interest in industrial automation due to its flexibility, mobility, ease of installation, and lower cost. Wireless systems, in general, require additional and different engineering and maintenance tasks, for example cryptographic key management for security. The pace of application in process control has been impeded, however, by concern about the risks involved in incorporating wireless paths in feedback loops and making the accommodations necessary for reliable control. The issue is that there are conflicts between maintaining control loop performance and the usual objectives in managing a wireless sensor network.**

In this paper, we take a holistic approach that addresses safety, reliability and security in two primary aspects: communication and control; thus we hope to contribute a more complete roadmap for developing safe and secure wireless networked control systems. This proposed framework represents a synthesis of two formerly separate bodies of research, one primarily focussed on communication requirements for safety and security and the other on safe and reliable controls.

I. Introduction

Distributed control systems that incorporate wireless networks, or what are called Wireless Networked Control Systems (WNCSs), are gaining in popularity. In such systems, distributed sensors, controllers and actuators exchange information over a wireless communication network. This interest is due to the many advantages achieved by replacing traditional point-to-point wired control architectures, such as reducing wiring costs, speeding deployment, facilitating installation and upgrade, and providing full or partial mobility and improved freedom in placing components [1]–[4].

Developing a WNCS is a challenge because it is necessary to satisfy pressing requirements in two primary areas: communication networks and control systems.

A. Communication networks

On the communication side concerns about reliability, security, integration, and lack of device interoperability have hampered deployment. To address these issues, WirelessHART [5], the first open and interoperable wireless communication standard especially designed for real-world industrial applications, was approved and released in 2007. In addition, ISA 100.11a is becoming a standard for process and factory automation [6]. Also, ZigBee [7] and various proprietary solutions [8], [9] are used for automatic metering systems.

Even though wireless communication offers many benefits, some wired fieldbuses will still remain in industrial communication systems for the foreseeable future. Therefore it is necessary to integrate these two technologies such that they interoperate seamlessly. This requires the development of an efficient and adequate solution for integrating wireless communication with existing fieldbuses and emerging field networks while supporting functional safety and security. This would enable an expansion of wireless sensor and actuator networks (WSANs) effectively into areas where wired communication has challenges with respect to cost, mobility, or physical degradation (e.g., mechanical wear, corrosion).

Most research done in the field of wireless extensions to traditional fieldbus communication fails to give a complete solution to efficient integration. This article outlines a complete framework for providing secure and safe communication in wireless / wired networks, first proposed in [10]. In addition, we present a solution to provide periodic and deterministic transmissions from gateway to actuators in a WirelessHART network, which is critical for use in control loops and was only recently devised [10].

Related communication-related background is outlined in [10], and specific references are given. This includes:

- How functional safety, security, and integration have been addressed in wired fieldbus communication with Profibus and Profinet,
- how wireless extensions of automation networks and fieldbuses have been researched and evaluated using an experimental industrial application layer protocol, multiple backbone routers and simulation tools,
- the possibilities of implementing Profibus DP on hybrid wired / wireless networks, based on Ethernet and Bluetooth, respectively,
- a performance comparison between the WirelessHART and ZigBee standards, showing that ZigBee is not suitable for use in wireless industrial control applications,

- an outline of IEC 62280-2, which presents functional safety and communication needs for open transmission systems [11], and
- standardization activities for integrating WirelessHART devices into Profibus / Profinet networks within Profibus.

Other supporting technology, e.g., Profinet IO, WirelessHART, Profisafe and the black channel principle, are also outlined in [10]. However, the main contribution is that [10] took a holistic approach to include safe and secure communications in a way not considered for standardization so far; we do the same in this presentation.

B. Control systems

The rapid development of micro-electro-mechanical systems and wireless communication technologies allow engineers to integrate small sensors, actuators, processors, batteries, and wireless communication devices into WNCSs. The introduction of wireless-in-the-loop produces control problems that are not encountered in wired systems.

We addressed these new control problems by developing a Wireless Networked Control System Coordination Agent (WNCSCA) to monitor the behavior of closed-loops with wireless links (sensor-to-controller, controller-to-actuator) and to coordinates with the WSAN to maintain acceptable performance [12]–[14] – this is a very important requirement for safe and reliable industrial control. Basically, although low data rates, network delays and packet losses are often acceptable or desirable in wireless communication networks, there are strict limits as to what can be accepted in the case of closed-loop control over a WSAN. This results in distinct tradeoffs between the requirements of network communications and control system performance.

Other researchers have addressed communication/control tradeoffs in a number of ways. Mazo and Tabuada [15] propose to let communication-based criteria dominate and limit the control action to an event-triggered implementation wherein control signals are kept constant until a process state violates a specified condition, at which time the recomputation of control signals is triggered. The resulting abrupt transients may not provide safe control, especially in nonlinear processes. Fischione *et al*. [16] present a protocol that optimizes WSAN energy consumption under constraints on reliability and latency of the packets, as dictated by the controlled process. This does not seem to provide an assurance that stability-related criteria are met, and it is inefficient in that the protocol does not take into account the mode of operation, e.g., steady state, set-point change or disturbance rejection. In steady state operation greater latitude in setting delay and data rate can be tolerated, for example, as long as the process is monitored to detect disturbances. Finally, a very conservative and theoretical approach is described in [17] in which discontinuous Lyapunov functionals are used to characterize admissible sampling intervals and delays that guarantee exponential stability.

In our first WNCSCA design the main control objective was maintaining a practical stability-related constraint, i.e., maximum acceptable percent overshoot. From the WSAN perspective, however, it is desirable to conserve energy and to have complete flexibility in configuring the network to promote the efficient use of resources; slower data rates and longer delays may result from achieving these goals. The main concerns were *path delay* and *data rate management*, both of which have a major impact on control system behavior and the efficient operation of the WSAN. The WNCSCA mediates between the needs of a supervisory control system and the WSAN gateway to allow as much network optimization, flexibility and efficiency as possible based on the safety and reliability requirements of the WNCS. Note that we assume that the gateway will be a powered node, with sufficient computational power and software to provide this functionality.

Outline: The remainder of the paper is organized as follows: In Section II we present a framework for safe and secure communication, and in Section III we outline an extension of WirelessHART to enable periodic and deterministic data transfer to actuators (which is critical in wireless control loops) and discuss the corresponding safety function response time. In Section IV we present a solution for control system safety and reliability. Finally, in Section V we conclude the paper. In essence, these contributions, we believe, forms a complete roadmap for developing safe, reliable and secure WNCSs.

II. Framework for Safe and Secure Communication

In wired fieldbus communication, most fieldbus protocols provide a safety protocol that can be used to fulfill functional safety requirements. Wireless technologies mostly come with a security solution, due to the nature of the open media. However, the security measures and capabilities are technology dependent, ranging from optional (ZigBee) to extensive and mandatory (WirelessHART). Using both wired and wireless fieldbus technologies to complement each other causes many new challenges, especially with respect to integration and maintenance, and also safety and security considerations, as illustrated in Fig. 1. In addition, the figure illustrates the gap between safety and security with respect to the media, i.e., there are no security measures in either the wired segments or wireless segments. It is of vital importance to achieve “seamless integration” of wired and wireless communication, to improve design, engineering, and maintenance efficiency. In industrial settings, different technologies will most probably be deployed even in the future, as it is extremely difficult to solve all industrial requirements with one standard / protocol. Therefore, we present a unified framework to deal with safety and security in heterogeneous networks, that hides the underlying technical differences.

We outline a framework based on the principle of the *black channel* in order to address safety and security issues in an integrated manner [18], [19]. In this way, each layer comprises all measures necessary to fulfill the safety or security requirements, without relying on services provided by other layers, thus reusing existing automation equipment and transmission protocols. The framework concerns equipment found in automation systems on the field network level, i.e., Programmable Logic Controllers (PLCs), Distributed Control Systems (DCSs), actuators, sensors, wired fieldbuses, and in addition wireless networks. Figure 2 illustrates the proposed method, where a security layer is added between the communication layer and the application

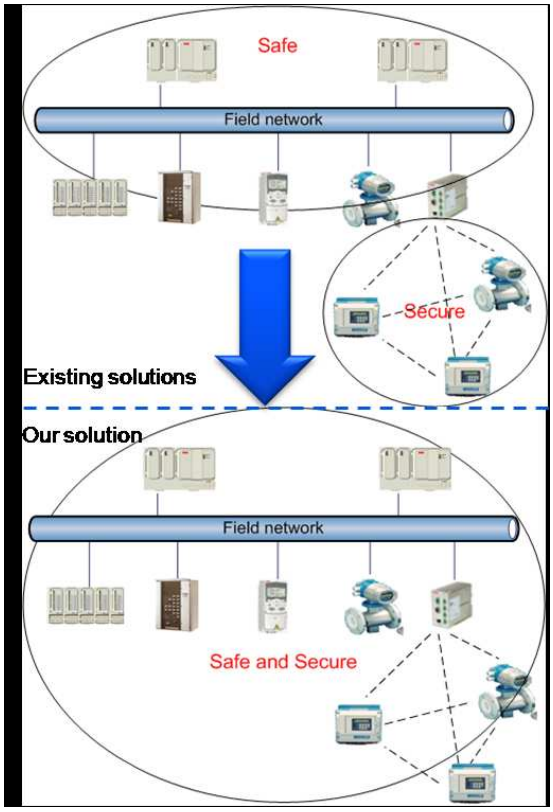

Fig. 1. The upper part of the figure illustrates current practice, where security is generally only considered in wireless communication and safety is considered in wired communication. The lower part illustrates the desired situation provided by the proposed framework, where safety and security are considered regardless of communication media

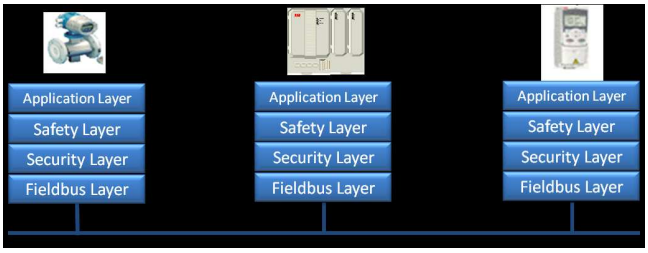

Fig. 2. The figure illustrates the proposed framework for safe and secure communication, where the Security Layer treats the Fieldbus Layer as a black channel, and the Safety Layer treats the Security and Fieldbus Layer as a black channel. Security and / or Safety can be added depending on the actual requirements and needs.

layer, using the communication layer as the black channel. The security layer is not added within the scope of the Open Systems Interconnection (OSI) model, but rather between the OSI model and the application to avoid conflicts with standards and to allow end-to-end security. In the same manner the safety layer is used between the communication layer or security layer, depending on the usage of the security layer. For safety certification reasons, the security layer is part of the safety layer's black channel. Within the proposed framework, safety and security layers can be utilized independent of each other and deployed based on the current requirements.

This approach enables end-to-end security as well as safety, without adding any safety or security requirements on the transmission media. It also suits both modular field devices such as distributed I/O's and compact devices such as field instrumentation. Within a modular device, the safety / security layers are deployed, using the device access point and backplane buses as a black channel. In the case of modular I/O, both safe, secure, and traditional I/ O modules can co-exist independent of the safety / security layers. This enables a broad range of applications where safety / security enabled devices can co-exist with already existing field devices. With this approach, the safety layer and security layer can be used independently and be deployed according to specific requirements. Furthermore, the safety and / or security layer can be deployed on a node-to-node basis, and co-exist on the same hybrid transmission system for full flexibility.

As in the case of safety protocols, our approach adds more or less redundancy in certain layers depending on the functionality provided by the black channel. The advantage of this is that the underlying technologies and standards belonging to the black channel do not have to provide specific functionality, as the upper layers do not rely on them. To exemplify, if a security layer is added, there will in some cases be a redundancy in the wireless segment, but the wired segment will be protected. The trade-off for end-to-end security could be partially overlapping security measures, but end-to-end security is achieved even if there is partial security in a subsystem, so a certain degree of redundancy with respect to security is desirable. For example, a common term in the context of security is *defense-in-depth*, i.e., several layers of security mechanisms are deployed to make it more difficult to bypass them. Again, this is transparent to the underlying transmission media.

III. Periodic Downlink Transmission in WirelessHART

The WirelessHART standard targets industrial control system applications, so we need to include actuators within WirelessHART, to enable it to be used in representative industrial control applications. Typically actuators require deterministic communication, thus best-effort communication as in the current standard is not sufficient in most cases.

A. Distributed Control Systems and WirelessHART

Traditionally, DCSs periodically acquire data from sensors, execute a control module, and finally send the output values to the actuators. Typical period times for DCSs in process automation range from $250\ ms$ to $1\ s$; however both faster ($10\ ms$) and slower ($5\ s$) sample times may be found. In cases where the period time is in the range of $10\ ms$ WirelessHART is not the technology to be used. In that case, a wireless interface for sensors and actuators (WISA) can be used; it is designed for update rates down to $10\ ms$ [20].

The WirelessHART standard defines a method to set up efficient and periodic data transfer ($\geq 250\ ms$) from a sensor to the gateway using *burst mode*. However, there is no definition for how to initiate efficient and periodic data transfer in the opposite direction (gateway to actuator). Using best-effort communication for distributing set-points for actuators in industrial control systems is far

from reliable. Also, to achieve good results from a control perspective, jitter and delays should be reduced as far as possible. All the set-points for the actuators need to be distributed back to the devices within the same cycle. WirelessHART allows the use of proprietary methods to add functionality, so it is possible to provide efficient data transfer from the gateway to actuator, something which current gateway/network manager vendors have not focused on.

B. Downlink Transmission Scheme

The solution proposed in [10] includes a new WirelessHART command that the control application can use to request periodic transmissions to be sent up to the actuators, using outgoing slots. A new WirelessHART command is necessary, as existing commands to initiate periodic transmissions assume that the network manager is the data sink. Since the typical period WirelessHART period is $250\ ms$ to $1\ s$ and a WirelessHART slot is $10\ ms$ one can easily deduce that the maximum number of successive slots for an access point ranges from 25 to 100 slots if all nodes have a direct link to the network manager, and use only one channel at a time given the radio constraints. If a DCS serves as many sensors as actuators, there will only fit 12 incoming slots for sensor data, and 12 outgoing slots for actuator data, given a period time of $250\ ms$, if all nodes have a direct link to the network manager. The WirelessHART standard permits communicating on 15 channels, so theoretically adding 14 access points could increase the number of available slots 15 times, if the access points are scheduled to communicate simultaneously on different channels in parallel.

The packet in the WirelessHART standard can only travel one hop per slot. This introduces delays for devices which are several hops away from the gateway. Another issue is that a device usually can only either listen for a packet or send a packet at one time. Relaying other devices' data will decrease the number of available slots, and could even increase the minimum allowed DCS period. Clustering the network is a solution which could reduce delays by creating simple one-hop clusters around several gateways, or access points if several are used. Thus proper planning of the architecture is important in order to create good network clustering.

One of the most important metrics for safety-critical applications is the time between a detected error and the transition to a safe state. In Profisafe, the Safety Function Response Time (SFRT) specifies the worst-case time before a safe state is achieved in the presence of errors or failures in the safety function [21]. Depending on the application, the requirements of SFRT range from milliseconds to seconds. This recently proposed downlink transition scheme [10] has been shown to reduce SFRT significantly, e.g., from $14.5\ s$ to $1.9\ s$.

IV. Framework for Safe and Reliable Control

The design of the original WNCSCA [12]–[14] was developed in the context of an intelligent agent-based supervisory control system called ICAM (Intelligent Control and Asset Management) [22], [23]. Some agents were developed for advanced control capabilities, e.g., linearized model identification (LMId) [24], fault detection, isolation and accommodation (FDIA) [24], [25] and nonlinear dynamic data reconciliation (NDDR) [26]. All of these agents were successfully tested on a high-order and highly nonlinear model of a three-phase gravity separator for crude-oil processing that had five control loops [27]. The ICAM system sends the low-level controllers signals such as set points, generalized binary noise for model identification, and control gains to tune controller performance.

When extension of ICAM to control systems with wireless paths in feedback loops was considered, it became evident that another agent was required to coordinate and mediate between the communications and controls functionality; hence the WNCSCA was devised. Here we present this agent in the same context, recognizing that it may be simplified considerably if other advanced control agents are not employed, in quite obvious ways. Furthermore, in this discussion we only show how to deal with control-loop data rates and path delays; the scope of this agent to handle more issues affecting control system performance, such as jitter, data drop-outs and wireless sensor network loading effects (e.g., variation of path delays with changes in data traffic) is certainly possible.

It must be emphasized that we assumed that the process with wired control loops already had a traditional "safety net" prior to the introduction of a WSAN, to deal with equipment malfunctions, operator error and other anomalies. The WNCSCA is designed to augment this "safety net", dealing only with the communication / control problems associated with closed-loop control over a WSAN.

During the operation of the ICAM supervisory system, it or its agents impose different requirements or specifications on the WSAN to complete their tasks properly. For example, ICAM may require different data rates for sensors and actuators in specific regimes, such as start-up, set-point changes, steady-state operation and disturbance rejection. During start-up mode, the initial process variable transients must decay under closed-loop control, so appropriate data rates and path delays must be imposed to ensure reliable operation (e.g., limited percent overshoot). Once the process reaches the desired steady-state set-point ICAM may invoke the LMId agent to perform model identification, perhaps using different data rates than before [24]. After that, the process may remain settled in steady state, in which case loops can be opened[1] and data rates reduced so ICAM can monitor the process; as long as there are no disturbances or set-point changes slow sampling can continue and the WSAN gateway can manage its data rates freely and thus operate efficiently. In many industrial systems a process may be in steady state for long periods of time, with infrequent set-point changes or disturbances requiring closed-loop control, so this strategy will allow the WSAN to be managed in a more optimal way much of the time.

In summary, the various modes of operation require tighter or looser constraints on data rates and path delays; the WNCSCA mediates between ICAM and the WSAN gateway to allow both the control system and the WSAN to meet their objectives as flexibly and safely as possible. The interface between ICAM and the WSAN gateway is

[1]Opening control loops momentarily to handle data drop-outs has been suggested in [2]; our strategy of opening control loops during steady-state operation to alleviate strict control-related WSAN constraints is new.

portrayed in Fig. 3; note that we assume the controllers are hosted on the same platform as the gateway, and the sensor / actuator (S / A) nodes are at the bottom of this figure. Here we describe the WNCSCA communication scheme; in [13] we presented and demonstrated the effective method and algorithm for determining the maximum allowable packet delays and minimum data rates that the WSAN gateway may utilize without excessively degrading the performance of control loops operating over the WSAN when loops are closed. Specifically, we define *design percent overshoot* (% OS) as desirable performance and *acceptable* % OS as the limit enforced by the WNCSCA; for example, the case presented in [13] corresponds to design % OS = 10, acceptable % OS = 25, which represents a case where fast response is more important than overshoot. More conservatively, one may use design % OS = 0, acceptable % OS = 10. The WNCSCA uses a nonlinear process simulator in an efficient way to determine the data rate and path delay safety limits for acceptable % OS.

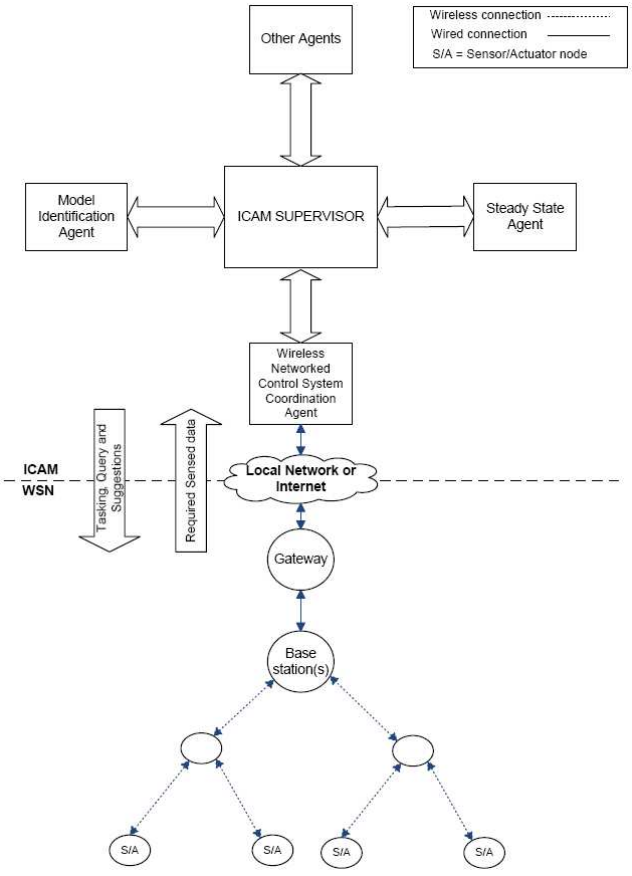

Fig. 3. Schematic of the WNCSCA interfaces with ICAM and a WSAN

A. WNCSCA Objectives

The objectives of this agent are as follows:

1) Manage energy consumption strategically, in partnership with the gateway, by allowing reduction of the data rates for sensor and actuator nodes as much as possible without degrading the performance of control loops,
2) monitor the process state to determine its behavior (mode), e.g., are the process variables in steady-state or transient conditions; this information is provided by ICAM's Steady-state Agent [26], and
3) conduct control performance analysis based on the path delay and sampling time of the WSAN; based on closed-loop path delays the WNCSCA will accept or reject a proposed WSAN configuration, and based on the control mode, e.g., open- or closed-loop operation, the lowest acceptable data rates will be specified.

B. WNCSCA Architecture

The functions and roles of the WNCSCA can be identified in different layers or levels, based on their functionality, as follows:

- **Node level**: this is the lowest level of work for the WNCSCA, where it is concerned with the data rate (sampling period) for each sensor / actuator node pair, which has a great impact on the energy consumption and the life time of the WSAN.
- **Network level**: this is the middle level of the WNCSCA's activity, where it is involved in specifying constraints on the management of the WSAN, such as the network configuration, path delay over sensor-to-controller and controller-to-plant paths, and connectivity.
- **Task level**: this is the highest level in the WNCSCA's effort, where it is involved in monitoring the WSAN, conducting performance analysis for the control system's loops, and assigning and coordinating sensing and actuation tasks.

C. WNCSCA Communication with ICAM and the WSAN gateway

The WNCSCA interfaces with the ICAM Supervisor and the gateway of the WSAN using new communication logic. This scheme can be divided into three phases, Start-up, Normal Operations and Abnormal Operations.

Start-up Phase (Booting and Initialization) – Note that we are assuming that the capabilities of the WSAN are conservatively adequate for control, so generation of an acceptable start-up configuration is assured; if this is not the case then we need to provide an escape to a FAIL SAFE mode if a suitable configuration cannot be found.

- **Booting**: During the booting process the three main entities, the ICAM Supervisor, WNCSCA and WSAN, represented by the gateway, start working for the first time. The operator starts operation via the ICAM Supervisor by sending a **`Start`** message[2] to the WNCSCA, as shown in Fig. 4. Each entity tries to make sure that the other partners are ready (existing and alive) by exchanging **`Wake Up`** and **`Hello`** messages.
- **Initialization**: In general terms, during the initialization process the WNCSCA commands the gateway to assess the health of the WSAN (see which nodes are operational, check battery levels and connectivity) and generate a proposed configuration for the WSAN; then the WNCSCA will check the proposed configuration based on a performance analysis for the nonlinear

[2]Actual messages are sent as integers; text is used here for clarity.

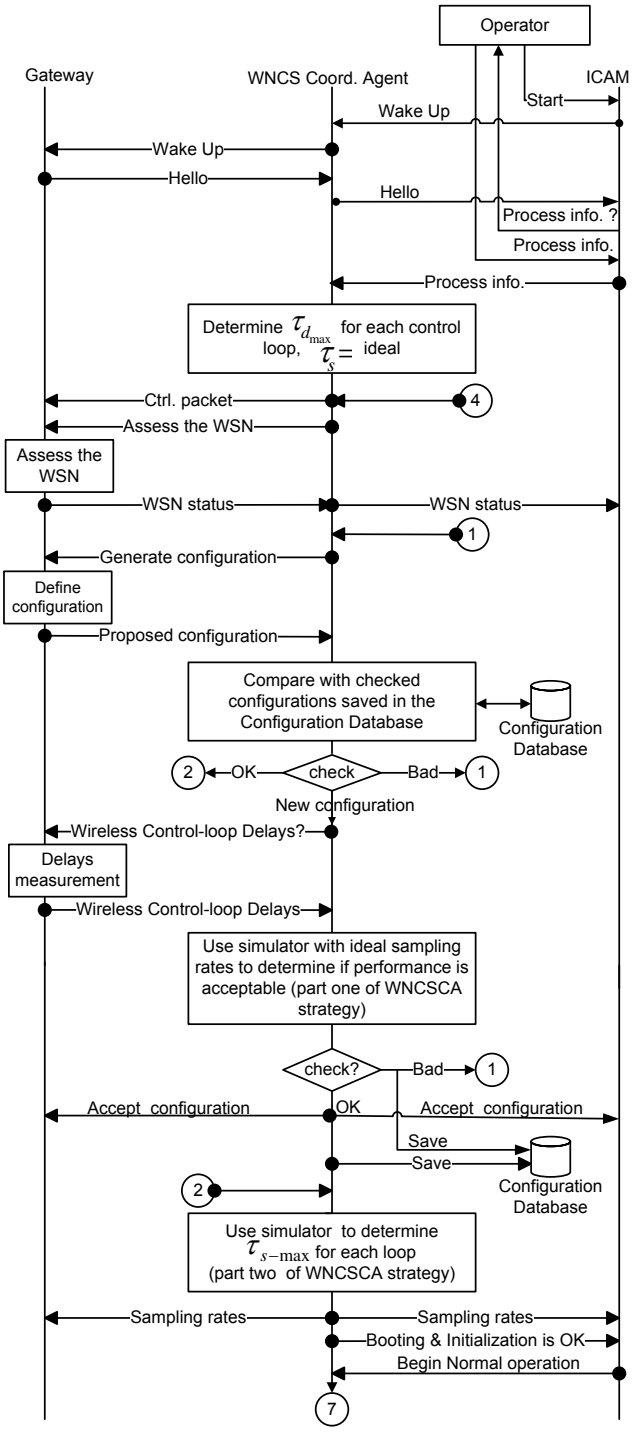

Fig. 4. WNCSCA communication scheme, Start-up Phase.

closed-loop control system over the WSAN, taking into consideration the sampling rates of sensor / actuator pairs and the time delays for WSAN paths in control loops. In part one of this process ideal sample rates (design values) are used to see if the WSAN delays are acceptable. In part two the slowest sample rate is determined such that acceptable control performance (acceptable % OS) is achieved; a simple relaxation method is used [13]. Based on that analysis, the WNCSCA will accept or reject the proposed configuration from the gateway; if rejected, the gateway must try again, decreasing the path delays (number of hops), as suggested by the WNCSCA. In the unlikely event that a suitable configuration cannot be found, the WNCSCA notifies ICAM, which in turn opens the control loops, escapes to a FAIL SAFE mode and raises an alarm. The Configuration Database which was implemented had a major impact on efficiently checking proposed configurations in a small amount of time. Also, note that **`Process info`** in Fig. 4 consists of the identity of the process to control, sensor and actuator node information (to specify the sensor and actuator node for each loop and provide ideal data rates), and set points to be used, and **`Ctrl. packet`** contains the sensor and actuator node and data rate information.

Normal Operations Phase – Normal operation of the WNCSCA is focused on monitoring the WSAN and maintaining acceptable control loop performance (defined in terms of the percent overshoot of the corresponding loop step responses). At the beginning of each cycle in this phase, the ICAM Supervisor commands the Steady-state Agent to perform a steady-state test, to see whether the controlled variables are operating in the steady or transient state. The WNCSCA checks if this is the first time for the controlled variables to operate in that state or not; in this way it detects the beginning of a steady-state or transient period for the controlled variables. If the new state is **`Transient`**, then the WNCSCA sets the data rates to values required for acceptable closed-loop control (Normal Sampling Rates, NSR) and tells ICAM to close the loops; otherwise, if the new state is **`Steady`**, the WNCSCA tells ICAM to open the loops and sets Reduced Sampling Rates, RSR, so the gateway can lower the sensor and actuator node data rates to be suitable for passive monitoring, including the detection of any subsequent start of **`Transient`** operation, thereby safely improving efficiency and reducing WSAN energy consumption as long as possible. The RSR should permit other ICAM activities such as Fault Detection, Isolation, and Accommodation (FDIA) [24], an important task during ICAM operation.

During normal operations, Fig. 5, the gateway may tell the WNCSCA that there are newly installed nodes, and the WNCSCA will relay that information to the ICAM supervisor. Then, the Operator must supply information which distinguishes between new sensor and / or actuator nodes, and identify any changed sensor and actuator loop pairs. The WNCSCA also forwards that information to the gateway, and the gateway may call for a new network configuration, which is handled as before.

Finally, the ICAM supervisor may decide that an "abnormal operation" is needed, i.e., a procedure that requires unusual resources, such as data rates that differ from start-up or normal (RSR or NSR). The WNCSCA checks in every execution loop of Normal Operations; if an abnormal operation is needed, then the ICAM supervisor sends an **`Abnormal Yes`** message to the WNCSCA and the WNCSCA will go execute the Abnormal Operations Phase (not shown), otherwise looping in the Normal Operations Phase continues. Note that the Abnormal Operations Phase is specific to auxiliary operations that the supervisory

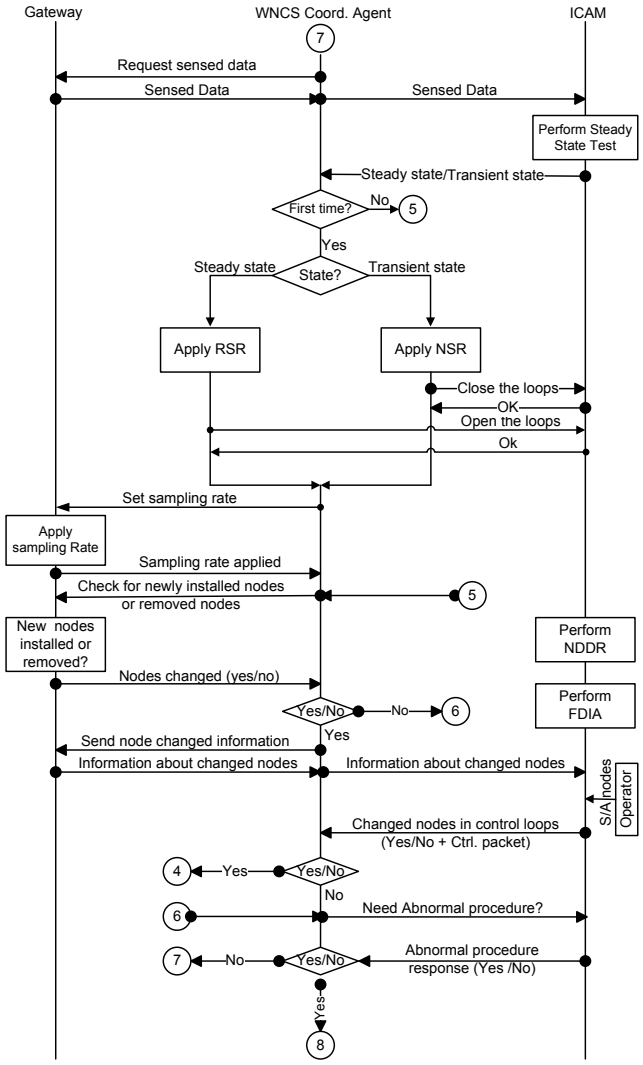

Fig. 5. WNCSCA communication scheme, Normal Operations Phase.

controller may decide to invoke, such as LMId, so we merely refer to [14] for an example of this phase. Once the "abnormal procedure(s)" are done the ICAM Supervisor will notify the WNCSCA that it may return to the Normal Operations Phase. As mentioned, this and other complicated logic / operations may be simplified or omitted in supervisory systems less complex than ICAM.

The WNCSCA was tested and simulated extensively with a real-time JCSTR simulator [28] in a variety of scenarios, to test the logic. These studies [12] successfully demonstrated the reliable and efficient operation of the WNCSCA and overall system.

V. Conclusion

A unified discussion of both the communications and control systems requirements for safe, reliable and secure wireless networked control systems is presented, as a path forward in the acceptance of WSANs for process control applications.

Communications: Using a wireless infrastructure as a platform for automation systems demands solutions which exist today in the wired case with the same properties, such as safety and security. Until [10] there existed no solution that considered functional safety for wireless sensor networks, and wired fieldbuses lacked security extensions within the context of industrial automation. The lack of these features would have become a severe problem, since scalable and modular solutions cannot be provided when integrating new wired / wireless devices into existing automation systems.

A solution to these difficulties is based on using the principle of the black channel and security modules, so safety and security measures can be deployed and co-exist in combined wired / wireless systems, depending on current requirements. A security module is a concept wherein a security layer provides measures for end-to-end integrity and authentication that can be retrofitted on existing automation systems. It has been demonstrated that this framework can be applied to an industrial automation system using Profisafe, Profinet IO, and WirelessHART.

It was clearly shown that periodic and deterministic downlink transmissions from the WirelessHART gateway to the WirelessHART actuation devices are needed, and WirelessHART has been extended to deal with this problem [10]. It was also demonstrated in that citation that this solution was viable for typical slower industrial processes requiring control sample rates in the order of a few seconds or more.

Controls: The WNCSCA described herein constitutes the high-level design and specification for a Wireless Networked Control System Coordination Agent to manage the potential "conflicts of interest" between industrial control systems requirements and objectives of typical WSAN gateway protocols. Care must be taken to maintain safe and reliable operation of the WNCS by teaming the WNCSCA with an existing safety net required for conventional wired control. The WNCSCA has been tested and simulated extensively with a real-time JCSTR simulator [28], and good results were obtained in terms of coordinating between the ICAM Supervisor and WSAN gateway and checking the effects of WSAN configurations on the performance of the closed-loop system.

The increased freedom given to the WSAN gateway to meet its objectives should depend on the current state of the control system loops that incorporate wireless paths. The novel communication scheme described here [12], [13] demonstrates that it is possible to significantly increase that freedom over other schemes [15]–[17] in a safe and reliable way.

In the current stage of development control-loop data rates and path delays were dealt with; we believe that these are the two most basic and important concerns. One may extend the scope of the WNCSCA to handle additional WSAN issues that impact control system performance, such as jitter, data drop-out and wireless network loading effects (e.g., variation of control-loop path delay with changes in network traffic).

References

[1] C. Fischione, K. H. Johansson, F. Graziosi, and F. Santucci, "Distributed cooperative processing and control over wireless sensor networks," in *Proc. International Conference on Wireless Communications and Mobile Computing*, July 2006.

[2] P. Kawka and A. Alleyne, "Stability and feedback control of wireless networked systems," in *Proc. American Control Conference*, June 2005.
[3] X. Liu and A. Goldsmith, "Wireless network design for distributed control," in *Proc. 43rd IEEE Conference on Decision and Control*, December 2004.
[4] N. Plopyls, P. Kawka, and A. Alleyne, "Closed-loop control over wireless networks," *IEEE Control Systems Magazine*, June 2004.
[5] (2010) HART 7 specification. [Online]. Available: http://www.hartcomm.org/
[6] (2010) ISA 100, wireless systems for automation. [Online]. Available: http://www.isa.org/isa100
[7] (2010) Zigbee alliance. [Online]. Available: http://www.zigbee.org
[8] L. Hardy and M. Gafen, "A new highly-synchronized wireless mesh network model in use by the electric company to switch to automatic meter reading: Case study," in *5th International Conference on Networked Sensing Systems*, June 2008.
[9] T. Zhong, Z. Peng, Y. Haibin, and W. Hong, "Zigbee-based wireless extension of foundation fieldbus," in *6th IEEE International Conference on Industrial Informatics*, July 2008.
[10] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Björkman, "Efficient integration of secure and safety critical industrial wireless sensor networks," *EUROSIP J. on Wireless Communication and Networking*, September 2011.
[11] *IEC 62280-2. Railway applications - Communication, signaling and processing systems - Part 2: Safety-related communication in open transmission systems*. International Electrotechnical Commission, 2002.
[12] H. M. S. Ibrahim, "Wireless networked control system coordination agent," Master's thesis, University of New Brunswick, March 2010. [Online]. Available: http://www.ece.unb.ca/jtaylor/Theses/Hazem_thesis.pdf
[13] J. H. Taylor and H. M. S. Ibrahim, "A new, practical approach to maintaining an efficient yet acceptably-performing wireless networked control system," in *Proc. 13th IEEE International Conference of System Science and Engineering, ICSSE 2010*, Taipei, Taiwan, July 2010.
[14] J. H. Taylor, H. M. S. Ibrahim, J. Slipp, and J. Nicholson, "A safe communication scheme for an intelligent wireless networked control system coordination agent," in *Proc. IEEE International Conference on Systems, Man and Cybernetics, SMC 2010*, Istanbul, Turkey, October 2010.
[15] M. Mazo Jr. and P. Tabuada, "Control over wireless sensor / actuator networks," *IEEE Transactions on Automatic Control*, July 2011.
[16] C. Fischione, P. Park, P. Di Marco, and K. H. Johansson, "Design principles of wireless sensor networks protocols for control applications," in *Wireless Network Based Control*.
[17] P. Naghshtabrizi and J. P. Hespanha, "Implementation considerations for wireless networked control systems," in *Wireless Network Based Control*.
[18] J. Åkerberg, "On security in safety-critical process control," Licentiate thesis, November 2009. [Online]. Available: http://www.iss.mdh.se/index.php?choice=publications&id=2081
[19] J. Åkerberg, F. Reichenbach, and M. Björkman, "Enabling safety-critical wireless communication using wirelesshart and profisafe," in *IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, Sept. 2010.
[20] J. Kjellsson, A. Vallestad, R. Steigmann, and D. Dzung, "Integration of a wireless i/o interface for profibus and profinet for factory automation," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4279–4287, Oct. 2009.
[21] *IEC 61784-3-3. Industrial communication networks - Profiles - Part 3-3: Functional safety fieldbuses - Additional specifications for CPF 3*. International Electrotechnical Commission, 2007.
[22] J. H. Taylor and A. Sayda, "Prototype design of a multi-agent system for integrated control and asset management of petroleum production facilities," in *Proc. American Control Conference*, June 2008.
[23] A. Sayda, "Intelligent control and asset management of oil and gas production facilities," Ph.D. dissertation, University of New Brunswick, May 2008. [Online]. Available: http://www.ece.unb.ca/jtaylor/Theses/Atalla_PhD_thesis_almost_final.pdf
[24] M. Omana, "Fault detection, isolation and accommodation using the generalized parity vector technique," Ph.D. dissertation, University of New Brunswick, October 2009. [Online]. Available: http://www.ece.unb.ca/jtaylor/Theses/Maira_PhD_thesis.pdf
[25] J. H. Taylor and M. Omana, "Fault detection, isolation and accommodation using the generalized parity vector technique," in *Proc. 17th IFAC World Congress*, Seoul, Korea, July 2008.
[26] R. del Pilar Moreno, "Steady state detection, data reconciliation, and gross error detection: Development for industrial processes," Master's thesis, University of New Brunswick, January 2010. [Online]. Available: http://www.ece.unb.ca/jtaylor/Theses/Pilar_thesis.pdf
[27] A. Sayda and J. H. Taylor, "Modeling and control of three-phase gravity separators in oil production facilities," in *Proc. American Control Conference*, July 2007.
[28] J. H. Taylor, "Jacketed continuous stirred-tank reactor - models, control systems and simulators," University of New Brunswick, Tech. Rep., November 2009.