LOGIIC
Wireless Project

March 2013

Final Public Report

Document Title	*LOGIIC Wireless Project: Final Public Report*
Version	*Version 2.0*
Primary Author	*A. McIntyre (SRI)*
Distribution Category	*LOGIIC APPROVED FOR PUBLIC DISTRIBUTION*
Approval Status	*APPROVED FOR LOGIIC USE*
Reviewed by AF Legal	*2013-03-27*
Approved	*2013-01-30*
Approver	*EC*
Digital Signature for PDF	*Signed by the LOGIIC EC Chair on March 20, 2013*

REVISION HISTORY

Version	*Author*	*Date*
1.0	A. McIntyre (SRI)	January 29, 2013
2.0	A. McIntyre (after technical editor review)	February 28, 2013

EXECUTIVE SUMMARY

LOGIIC[1] was established by members of the oil and gas industry in collaboration with the Cybersecurity Research and Development Center (CSRDC) of the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T) to review and study cybersecurity issues in Industrial Automation and Control Systems (IACS) impacting safety and business performance as they pertain to the oil and gas sector. LOGIIC has sponsored research initiatives that involve the interests of oil and gas sector stakeholders.

IACSs are managed from control centers with a number of interconnected networks, field devices, and handheld devices that are used by internal, external, employee, and contract users. From the control center, operators maintain a current view of parameters relevant to the operation of the plant, facility, field, or pipeline. Operators at the control center issue commands to final elements, taking into account the monitoring from field devices. Automation vendors are offering new solutions that potentially expand the use of wireless technologies that can be used for monitoring and control.

The objective of this project was to assess the cyber security of wireless devices, taking into account the security and security operability in terms of availability, integrity, and confidentiality. The study included background research and a hands-on assessment of an automation vendor's available wireless technology offerings. Using test scenarios, the project assessed security control functionality, interoperability, system availability, confidentiality, and integrity. The project's findings seek to increase knowledge of security boundaries, operability, and maintainability of the available wireless technologies.

The many facets of implementing security on a wireless network include the join process, key handling, cryptography, and device configuration. Implementing security across these areas is needed to ensure the confidentiality, integrity, and availability required to perform control functions securely over a wireless network. If security is layered and well implemented across the wireless network, attacks will require significant resources and time.

Given the security of wireless networks and the join process, more attacks are available to simply deny connectivity rather than attacks with data change or pointed consequences. While man-in-the-middle attacks may be more difficult on a well secured network, many threats to the wireless network exist that can create denial of service and connectivity results. These include deauthentication ("deauth") attacks, advertisement packet spoofing, and jamming. Jamming is perhaps the most difficult to prevent. This study focused on the recoverability of devices after jamming attacks and, in many cases, devices recovered without issue. In this assessment, the join process and network security to protect against the outsider threat is sound. Insider threats, as expected, have a greater ability to do harm, but additional risk mitigations keep consequences minimal. Jamming attacks, as expected, are successful even with integrated security. Wireless devices recovered well from jamming attacks and recover with minimal interaction after deauth attacks.

Given the fact that wireless networks can be subject to significant denial-of-service attacks as well as man-in-the-middle attacks, situational awareness is necessary to detect rogue APs and devices and general network health. Intrusion detection capabilities can be positioned to monitor for insider and outsider threats. This monitoring can provide more insight into behaviors on the network in a timely manner, instead of an operator realizing a loss of data view on a device that may only report back to the control system periodically.

[1] LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity.

Many field devices report data back to the control systems over the wireless network (e.g., control capability occurs on handheld devices for mobile operators on a plant floor). In addition to wireless network security, additional access controls and policies on the handheld devices can ensure that control functions are not exploited through easy access of distributed systems.

Like all network security methods, patching and updating are necessary to maintain a high level of security. A changing threat landscape and the increased commonality of the Wireless Highway Addressable Remote Transducer (HART) protocol requires the maintenance of strong security such as key maintenance and protection, system updates, and risk mitigation. Over time, it is expected that WiFi will continue to be an attractive target and Wireless HART may become more common. This will result in advanced attacks and toolkits available to the adversary. Asset owners must continuously maintain due diligence related to security of wireless networks based on the changing threat landscape.

The risks associated with performing control over a wireless network should be matched against the corporate operational risk profile. Considerations should include the implementation of security at all levels of the wireless network, patching and maintenance, and the structure of the network join process. Because jamming and other denial-of-service attacks can cause non-permanent loss of control and loss of view, utilizing wireless for control functions should be considered carefully before implementation. Using wireless with control functions would likely be limited to noncritical applications that are not impacted by potential delays from jamming. Wireless is not recommended for safety functions.

Contents

List of Tables

List of Figures

DISTRIBUTION

This report is approved by the U.S. Department of Homeland Security and the LOGIIC Executive Committee for unlimited public distribution.

ABSTRACT

LOGIIC[2], established by members of the oil and gas industry in collaboration with the Cybersecurity Research and Development Center (CSRDC) of the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T), sponsor research initiatives that involve the interests of oil and gas sector stakeholders.

Industrial Automation and Control Systems (IACS) are managed from control centers with a number of interconnected networks, field devices, and handheld devices that are operated by internal, external, employee, and contract users. From the control center, operators maintain a current view of parameters relevant to the operation of the plant, facility, field, or pipeline and issue control commands to final elements, taking into account the monitoring from field devices. Automation vendors are offering new solutions that potentially expand the use of wireless technologies that can be used for monitoring and control.

The objective of this project was to assess the cyber security of wireless devices, taking into account the security and security operability in terms of availability, integrity, and confidentiality. The study included background research and a hands-on assessment of an automation vendor's available wireless technology offerings. Using test scenarios, the project assessed security control functionality, interoperability, system availability, confidentiality, and integrity. The project's findings seek to increase knowledge of security boundaries, operability, and maintainability of the available wireless technologies. This report discusses the assessment attributes, findings, and considerations for using wireless in process control environments.

[2] LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity.

ACKNOWLEDGMENTS

The project to evaluate wireless technologies was developed and guided by the members of the LOGIIC, who devote their time and expertise to conducting projects that will lead to cybersecurity improvements in the oil and gas industry, and in the IACS community in general. LOGIIC would like to thank the U.S. Department of Homeland Security, Science and Technology Directorate, for providing leadership, vision, and commitment to enhancing cybersecurity. The Automation Federation serves as the LOGIIC host organization and provides a needed home and legal framework for our efforts. We would also like to express our appreciation for the work of our team of subject matter experts who refined the evaluation strategy, performed the system evaluations, and developed the project reports. Since the inception of LOGIIC, the scientific research organization SRI International has provided coordination, project management, and subject matter expertise.

The work performed on this project by SRI International and its subcontractors was funded under contract by the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate. The content is solely the product of LOGIIC and does not necessarily represent the official views of DHS.

1 Introduction

LOGIIC was established to review and study cybersecurity issues as they pertain to the oil and gas sector, and has sponsored research initiatives that involve the interests of oil and gas sector stakeholders. LOGIIC initiatives are applicable to many industries with control systems.

Industrial Automation and Control Systems (IACS) are managed from control centers with a number of interconnected networks, field devices, and handheld devices that are operated by internal, external, employee, and contract users. From the control center, operators maintain a current view of parameters relevant to the operation of the plant, facility, field, or pipeline and issue control commands to final elements, taking into account the monitoring from field devices. Automation vendors are offering new solutions that potentially expand the use of wireless technologies that can be used for monitoring and control.

The objective of this project is to assess the cyber security of wireless devices, taking into account the security and security operability in terms of availability, integrity and confidentiality. The project considers the automation vendor's ability to maintain security features through the lifecycle of the automation solution. The project included background research and a hands-on assessment of an automation vendor's available wireless technology offerings. Using test scenarios, the project assessed security control functionality, interoperability, system availability, confidentiality, and integrity. The project's findings provide each LOGIIC member company with the knowledge of security boundaries, operability, and maintainability of the available wireless technologies.

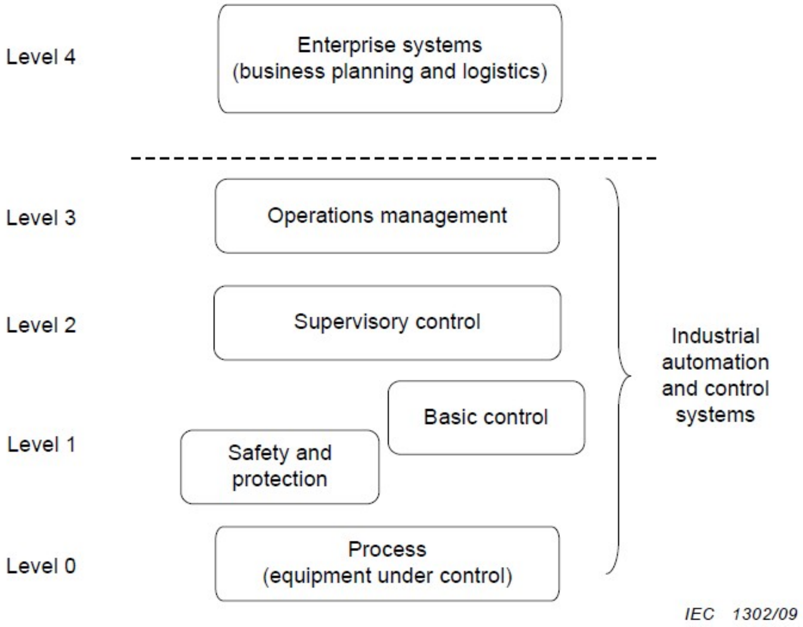
This report presents overarching conclusions on the use of wireless technology in an IACS environment. These conclusions are a result of technical assessment and analysis. Technical viability, implementation, maintenance, and usability were all considered in determining the level of security available in wireless technologies. This report aims to (1) convey important factors in the consideration of wireless technology in an IACS environment and (2) support a dialogue between asset owners and automation vendors.

1.1. Intended Audience

The intended audience for this report is the IACS technical and security communities; automation vendors, and security vendors.

2 Project Background

When defining this project, the LOGIIC members chose to scope the assessment of wireless within the areas defined in the section below. This project includes wireless technologies used with equipment and integrated systems that are part of Level 0, 1, 2, and 3 with their extension into Levels 3.5 and 4 (see Figure 1). (Safety systems were not included in the assessment phase of this project.)


Level 4
Enterprise systems (business planning and logistics)
Level 3
Operations management
Level 2
Supervisory control
Level 1
Basic control
Safety and protection
Level 0
Process (equipment under control)
Industrial automation and control systems

IEC 1302/09

Figure 1 Reference Model, IEC 62443 Standards

Wireless solutions were considered within various categories (control and monitoring) and classes (0 to 5) of process control applications (Table 1).

Category	Class	Application	Description	Importance of message timeliness increases ↑
Safety	0	Emergency action	(always critical)	
Control	1	Closed loop regulatory control	(often critical)	
	2	Closed loop supervisory control	(usually non-critical)	
	3	Open loop control	(human in the loop)	
Monitoring	4	Alerting	Short-term operational consquences (e.g., event-based maintenance)	
	5	Logging and downloading/uploading	No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)	

Table 1 Use Categories and Classes

The wireless configuration in this assessment was an integral part of the control system architecture. The focus of the assessment was the wireless functionality, and the control applications were not the primary target.

To meet the project objectives, a vendor selection process was established, candidates were evaluated, and selections were made based on established criteria. Likewise, a selection process was established for a wireless subject matter expert to conduct the hands-on testing during the assessment phase. An assessment was conducted using vetted methodologies and approaches. Technical results were collected, analyzed, and documented. This report presents the overarching conclusions regarding wireless technology in an IACS environment that were generated through this assessment and analysis process.

3 Technical Approach

A great deal of previous research and analysis exists for the security implications of using wireless technologies. The LOGIIC project conducted significant background investigation into the use of Wireless HART, WiFi, ISA 100 standards, and existing product offerings to scope the overall analysis. Evaluation criteria and core objectives, such as the ability to securely conduct control over wireless in an operational environment, shaped the technical approach and evaluation process.

3.1 Assessment Methodology

After selecting an automation vendor and wireless subject matter expert (SME), a Test Plan was drafted that included a detailed approach, rules of engagement, defined scope, and assessment objectives. The automation vendor's wireless solution was installed in a test lab in June 2012, and the full assessment occurred in July 2012.

This assessment was considered a partial-knowledge assessment that considers both insider and outsider threats. Although the assessment team had publicly available documentation on the wireless architecture, no insider access was provided prior to the assessment.

During the project planning phase, the LOGIIC technical team defined the following devices and components to be within the scope of the project:

- Wireless controllers
- Field devices
- Wireless to wired gateways
- Wireless video
- Handhelds and mobile devices
- Sensor networks

The assessment of these devices within the test lab environment used different attack vectors and approaches to determine the security of critical processes and services. The architecture under test represented a typical IACS environment that included a control center, plant environment, field system, and all networking. Safety systems were not included.

The scope of this assessment was based on the objectives of the LOGIIC wireless project. Standard assessment approaches, such as test cases, were used in conjunction with the standard risk equation to ensure all testing expresses a plausible threat. Risk is characterized in terms of threat, vulnerability, and consequence. Only plausible threat vectors and those identified within the rules of engagement were tested. The following high- level steps were followed during the assessment for each device or system of devices:

1. Reconnaissance
2. Information capture/data retrieval attempts
3. Pointed attack
4. Denial of service

The attack methods and techniques employed in the assessment align with overarching project objectives: Confidentiality, Integrity, and Availability (Table 2).

Technique	Meets Objective			Notes
	Confidentiality	*Integrity*	*Availability*	
Packet Capture	X			
Packet Injection		X		
Session Hijacking	X	X		
Man-in-the-middle	X	X		
Packet Spoofing		X		
Packet Replay	X			
Fuzzing		X	X	
Denial of Service			X	
Limited Jamming			X	
Recon & Research				Pre-work only, info gathering

Table 2 Assessment Objectives

3.2 Assessment Approach

As with all standard assessment approaches, attacks were deemed successful only if they were traceable and reproducible. Specific test scenarios and attack vectors were selected to reflect a plausible threat.

Upon completion of the architecture setup, the SME performed reconnaissance activities on the network and selected comprehensive test vectors to represent insider and outsider threat within the list of acceptable techniques identified above. The selected test vectors included:

- Jamming
- Deauth attacks
- Packet capture and decomposition
- Recognized rogue access point
- Denial of join, joining spoofed network (advertisement attacks)
- Join analysis, crypto analysis, investigation of security implementation
- Trusted insider attempts (scanning, rogue access point attempts)

For each wireless network, tools were employed to test the specific test scenarios listed in Table 3.

WiFi	Wireless HART
Connecting Monitoring Scanning Probing Attacking Custom scripts Flooding Deauth Rogue access points	Monitoring Packet investigation Rogue gateway and devices

Table 3 Scenarios Based on Network

These tools are readily available to the public free or for purchase, and therefore available to any adversary. (Tables 4 and 5) Some custom scripts were also developed and used during the test scenarios.

Connecting	Monitoring	Scanning	Probing	Attacking
airmon-ng wpa_passphrase wpa_supplicant iwconfig ifconfig	airodump-ng wireshark	nmap zenmap nessus ocs cisco-password-scanner nipper	netcat ssh putty ftp browser ping	ettercap-ng mdk3 aireplay-ng airbase-ng spike metasploit cisco-global-exploiter

Table 4 Tools & Commands Used for WiFi Testing

Monitoring	Packet Investigation	Rogue Gateway and Devices
Wi-Analys Ubiqua	SCAPY CCM* AES Utility	TI ZigBee Development Kits Awia-Tech Dust Networks

Table 5 Tools used for Wireless HART Testing

The assessment was completed over the course of 2 weeks. The wireless SME assessment team split into groups that focused on each vector or target network (i.e., WiFi team, Wireless HART team, jamming team). The results of the assessment were combined with project research to form conclusions about the use of wireless in a control environment.

3.3 Analysis of Findings

Findings and conclusions included consideration of multiple data sources:

- Background research conducted under the project
- Engagement with wireless experts across industry and research laboratories
- Product documentation from the automation vendor
- Assessment test scenario results
- Background information on each threat vector provided by the SME
- Observations during the assessment
- Usability testing

The assessment included testing on a large, complex wireless architecture. Security of the wireless capability was the main objective, but consideration was also given during the testing to the ease of setup, uptime and connection stability, system complexities, usability, and network join times. The SME assessment team, automation vendor, and LOGIIC technical leadership worked together to form overarching conclusions. A consensus was reached among all participants on these findings, which are discussed in Section 4.

4 Assessment Findings

The findings enumerated in this section offer conclusions about the use of wireless in an IACS environment.

4.1 Wireless Attack Vectors and Threats

Wireless networks often make attractive targets, in part because of early, less secure protocols. The shift to using wireless for critical operational systems has warranted caution from the industry. In general, industry seeks to facilitate operations and make core processes more efficient. However, this desire must be balanced against security and confidence in the technology. Much depends on implementation of the wireless network, as discussed later in this report, and threat resources. Although wireless may be a more attractive target, it is not necessarily an easier target if it is implemented securely.

4.1.1 Insider and Outsider Threats

Threats to wireless networks, like all networks, can be characterized as insider or outsider. It can be assumed that insider threats can do more damage than outsider threats. Insider threats to the wireless network indicate a successful exploitation of a vulnerability to perimeter security or access to the network join key. The assessment conducted under this project spent equal time testing outsider and insider threat vectors. Several factors must be considered when characterizing threats to wireless networking, specifically in an IACS environment.

WiFi networks may be more well-known in the threat community than Wireless HART networks. Unlike a common wireless network or public hot spot, adversaries would require reconnaissance of the network or some background information on an IACS network in order to exploit control functions on the wireless network with speed and stealthiness (that is, if the wireless network is implemented securely). A threat may select an easier vector if the goal of attack is a specific manipulation of a control function. As discussed in the following section, denial-of-service attacks on wireless networks may be an exception.

Available tools to exploit and attack wireless network are plentiful. However, advanced attacks on cryptography, man-in-the-middle, and detailed fuzzing attacks require significant resources and time. Sophisticated Wireless HART toolkits that assist in attack scenarios do not yet exist. It is assumed, however, that like all networking technologies, available attacks, malcode, and toolkits will become more readily available over time.

Preventing outsider threats requires careful implementation of the wireless network, including a sophisticated join and re-join process, a successful cryptographic implementation, and well-planned layered defenses. Likewise, these controls must be maintained and updated as new threats arise. Trusted insider testing (with the join key provided) conducted during the assessment provided findings for the team to analyze. Trusted insiders had the ability to join an undetected rogue device to the network, map the network, and scan for potential vulnerabilities. Preventing insider threats is highly dependent on those layered controls with role-based access, and in some cases physical security. An insider threat often has the ability to map the network and fingerprint systems. They may also leverage devices on the network, including those with common vulnerabilities that are reliant on perimeter security for protection. Network flooding is particularly efficient in disrupting the network as an insider. Lastly, detecting an insider threat is highly dependent on network monitoring. Devices join and rejoin the network periodically, which can mean situational awareness and joins to the wireless network are not often monitored. Awareness of rogue device presence or network anomalies is important in preventing damage by an insider threat.

4.1.2 Denial of Service

Denial-of-service attacks can be a reality for all networks, but wireless networks are also subject to jamming, making denial of service an increased concern. Denial-of-service attacks also require less reconnaissance and knowledge, and at times fewer resources, if simple disruption is the objective of the attack. Deauth attacks, jamming, network flooding, and fuzzing are all examples of denial-of-service attacks explored during the assessment conducted under this project. Each is discussed in detail under Section 4.3, but it should be recognized that denial of service is a significant threat vector to wireless and should be considered, given critical operations that may be conducted over the network.

Denial-of-service attacks are difficult to prevent, but in many cases during the assessment process, devices and the network itself recover once the attack is stopped. In these cases, a persistent threat is required to utilize resources and risk their identification for extended periods of time to create a relatively low consequence.

4.1.3 Man-in-the-Middle

Successful man-in-the-middle attacks require penetration of the network as an outsider, or insider access. Also required are sophisticated tools, an understanding of the network, and an exploitable vulnerability. In many cases, attacks must be focused on lower network levels using a sophisticated attack vector. For example, Wireless HART packet injection and man-in-the-middle attacks are highly complex, are resource and time-intensive, and require toolkits not yet readily available. While man-in-the-middle attacks have more pointed objectives than denial of service, they also require more effort and resources. During the assessment conducted under this project, well-implemented security on the wireless network prevented successful man-in-the-middle attacks.

4.2 Wireless Implementation – Security Considerations

A significant finding from the research and assessment activities is importance of the implementation of security within the wireless network. Several elements within the network must be secured according to standards or highest available protection levels to ensure the entire viability of the network. These elements are discussed below.

4.2.1 Network Join Process

During the assessment, significant research was conducted on the network join process, join packet, network timing, and cryptography. The use of network and session keys, join key rotation, and key structure, protection, and use policies all contribute to the overall security of the network. Incorrect implementation of these can create exploitable weaknesses in the network, offering an avenue of attack by an outsider. During the assessment, an investigation of the join process and key structure on the test lab architecture concluded that the network security was strong and implementation was thorough, with layered security. The SME's investigation thoroughly considered all aspects of the join process and the cryptography. All findings indicated that the network join process was sound and well planned. For example, the join key rotation process was secure, a common and current key for the join and rejoin process was used, and the session and network keys were encrypted. As a result of the test, it was determined that an outsider would not be able to join the network without a join key. Therefore, handling and protecting the join key within the organization is important. Join keys for Wireless HART are shared out-of-band and require physical access to the device. All session keys are sent encrypted using the join key. Proper methods should be used to destroy or clear devices before they are discarded to protect join and session keys on the device. Security of Wireless HART network is based on protection of keys and the AES-128 algorithm. With no join key provided, attack vectors from the outsider would be highly sophisticated and require toolsets that do not yet exist.

This assessment finding indicated the overall importance of securing the join process. Join key rotation and the entire join process illustrate extensive planning in the implementation of security throughout the process. Asset owners that choose to implement a wireless network should fully explore or test the join process within an offered solution. Given the criticality of the join process in the overall security of the network, significant emphasis should be placed on evaluating the join process prior to implementation.

As expected, jamming can prevent a device from joining a valid network. Jamming was the only test vector able to compromise the join and impact availability. Jamming is discussed in later sections of this report.

4.2.2 Cryptographic Attributes

The assessment verified that the wireless network under test used encryption for the join key and session key. Careful implementation of cryptography throughout the join and rejoin process is important to ensure no exploitable weaknesses exist. For example, the SME conducted an extensive investigation of the Nonce[3] process on the Wireless HART network. Analysis of the cryptography implementation concluded that the Nonce process was highly secure. Mishandling the Nonce can create a vulnerability to replay attacks and add to the plausibility of breaking the encryption. It was concluded that successful completion of an attack exploiting the cryptography and injecting a packet would be extremely resource-intensive, with possibly an improbable chance of success. This results in the conclusion that on a wireless network with a secure join process, analyzing and breaking well-implemented cryptography is an unattractive and unlikely threat vector.

4.2.3 Network Resilience

In addition to the secure implementation of the join process, cryptography, and key handling, overall resilience of the wireless network is a consideration when conducting critical operations. Discussed further in Section 4.5, wireless networks can be subject to threat vectors creating denial of service and connectivity. Device recoverability and the rejoin process must be sound and tested to ensure the network recovers after a denial of service.

4.3 Common Attack Vectors

The assessment conducted under this project tested insider and outsider threat vectors. These vectors were selected based on the scope and objectives defined in the project. Readily available tools, custom scripting, and common exploits were used collectively to assess the security of the wireless network and understand the impacts of specific vectors.

4.3.1 Ad Packet Spoofing

During the assessment, significant testing was conducted using spoofed network advertising packets. Bombardment of false advertisements can prevent a wireless device from connecting to a valid network. This was demonstrated during the assessment. A wireless device under test attempted to join the rogue network, but did not actually connect. During the assessment, this attack was successful at denying

[3] Nonce ("Number Once") is a random number used in cryptography as part of the authentication process. The implementation of the Nonce, its use with the join key, and mathematical derivation should all be done correctly to ensure the authentication process is secure.

service to a device that had not yet joined a valid network. Note that this does not affect devices already joined to the valid network. The finding from the test indicates that a device may be prevented from successfully joining a valid network, but a persistent threat is continually bombarded with false advertisements. When the bombardment stops, the device joins its valid network.

4.3.2 Rogue Access Points

Establishing rogue access points is a common threat vector to wireless networks. Implementation of layered security on the network can prevent a rogue access point. During the assessment and testing timeline, the SME team was unable to successfully establish a rogue access point on the wireless networks. Given the security of the join process and cryptography employed on the test networks, it is unclear whether a rogue access point could be established with significant resources or time.

4.3.3 Fuzzing

Fuzzing is another common threat vector to wireless networks. Fuzzing, or directed flooding of specific packets, can require significant time and resources to accomplish. Rather than a simple denial of service, fuzzing is often more structured to uncover specific vulnerabilities such as buffer overflows. Correctly implemented security on a wireless network can prevent fuzzing. During the assessment, attempts were made to fuzz the Wireless HART network, but were unsuccessful. The network under test was not vulnerable to this type of attack within the testing timeline, and due to the security employed on the network, the SME could not calculate a timeline to create a successful fuzzing attack.

4.3.4 Jamming

In the project planning phase, LOGIIC determined that limited time would be spent on jamming tests as it is expected that all wireless devices are susceptible to jamming. This was validated during the assessment. Other results from the jamming tests included data on the recoverability of devices after jamming is stopped. For example, field devices under test recovered immediately after jamming was stopped. Older handheld devices required interaction, such as rebooting or resetting of the network interface card. New handheld devices recovered immediately.

It was also observed that the effect of jamming on the handheld displays makes it appear that the device is out of range. Unless equipment to detect jamming is in place, it is difficult to distinguish jamming from other network problems. Also, physical proximity of primary and backup systems should be taken into account. Jamming at a distance will likely affect systems in very close proximity in the same way.

It was determined during the assessment that controllers on the test network required a large amount of RF to successfully jam, whereas Wireless HART devices can be a prime target due to their lower power output. The equipment required to create a powerful enough jammer to target Wireless HART devices from a distance is sufficiently simple to definitely constitute a realistic threat. The SME calculated the estimated cost to jam Wireless HART devices from a distance of 1 km (0.6 miles) is $1,000.

4.3.5 Deauth Attacks

Deauthentication, or deauth attacks, use well-known tools such as Backtrack and Airodump in an attempt to deauthenticate and deny access to specific devices on the network. During the assessment, deauth attacks were conducted against devices on the WiFi network. These attacks were successful in denying connectivity to the devices under attack, which resulted in data view loss. As with jamming, when the deauth attack was stopped, some devices recovered without interaction, while some required network diagnostics or even a reboot. Deauth attacks can be successful denial-of-service attacks that result in the need for manual interaction with devices to recover their functionality.

4.4 Summary of Technical Findings

Given the complexity of the test vectors and the amount of time required to complete specific tests, the technical results have been categorized by vector, as summarized Table 6.

Technical Finding	Availability	Confidentiality	Integrity
Network Join Process	Not Affected	Not Affected	Not Affected
Jamming	Affected (1)	Not Affected	Not Affected
Deauth attacks	Affected	Not Affected	Not Affected
Advertise Packet Spoofing	Affected	Not Affected	Not Affected
WirelessHART Nonce Investigation	Not Affected	Not Affected (2)	Not Affected (2)
Wireless HART Packet Injection	Not Affected	Not Affected	Not Affected
Manual Fuzzing	Not Affected	Not Affected	Not Affected
Rogue Access Point	Not Affected	Not Affected	Not Affected
Trusted Insider Testing	Affected	Affected	Affected
Intrusion Prevention	Not Affected	Not Affected	Not Affected

Notes:
1 - Jamming was highly effective at disrupting availability of wireless components.
2 - Nonce process is secure as long as the same Nonce never repeats by rotating the encryption keys.

Table 6 Technical Findings

4.5 Technical Considerations

The SME, automation vendor, and LOGIIC assessment team developed a list of technical considerations when implementing a wireless network. Asset owners are encouraged to discuss these considerations with their automation vendor when selecting and implementing a wireless solution.

4.5.1 WiFi vs Wireless HART

On the architecture under test, setup and implementation of the WiFi network was more time-consuming and resource-intensive than setup of the Wireless HART network. Both networks were impenetrable by the SME testing outsider threat vectors. More toolkits exist to target WiFi networks than Wireless HART, making Wireless HART packet injection and man-in-the-middle attacks highly complex, as well as resource- and time-intensive.

4.5.2 Intrusion Detection and Monitoring

As in a wired network, intrusion detection and monitoring is an important element in network security. This is the case from a network management perspective as well as an operational view. Because denial of service and loss of connectivity is a common goal of many existing threats to wireless networks, situational awareness is a method of identifying systems under attack. For example, field systems may only provide data back to the control system periodically. Situational awareness on the operator console can be uninformative during an attack. The system would not typically be processing data in a way that would distinguish certain network events. In that case, some types of attack look like legitimate activities and the operator is unaware of the events under way. An intrusion detection system may identify rogue access points, general network health problems, and other threats before an operator realizes that one or more devices have lost connectivity.

4.5.3 Supply Chain Viability

Wireless networking solutions often contain a number of field devices, handhelds, and access points. Implementation of security on the wireless network requires consideration of device configuration, protocols, encryption, the join process, and many other attributes. An assessment of layered security is often required when considering a full implementation of wireless networking. Asset owners conducting control functions over wireless should be provided with a clear understanding of security mechanisms implemented across all components and the entire solution. If the solution being considered includes devices from other manufacturers, an asset owner should be provided with (1) assurance from the automation vendor that security is comprehensive, (2) detailed documentation of the join process and security layers, and (3) confirmation that the solution meets export control guidelines.

4.5.4 Wireless in Network Security and Control Isolation

Reachback to control systems from the wireless network should be protected through network security controls. Like all field networks, layered access to control systems can be ensured through firewalls, VPN, role-based access control, and other mechanisms recommended in industry standards and guidelines. Security of data transmitted from field devices must be employed to ensure integrity of data used to make control decisions.

4.5.5 Handheld Devices for Mobile Operators

Handheld devices on the wireless network may have the ability to perform control functions. This can make the handheld devices more critical assets than field devices that simply provide data readings. Role-based access control, physical security, and use policies can be considered to provide additional protection. Wireless network security may be secure, but significant insider threat risks may be present if a handheld device is left unattended without a user log-out or screen lock.

4.5.6 Resource Requirements

Prior to selecting and implementing a wireless solution, asset owners should consider their architectures, risk portfolio, and resource availability for maintenance activities. For example, key questions for the automation vendor or solution provider could include:

- Will the asset owner or automation vendor install the wireless network?
- Who will maintain the wireless network?
- Will the asset owner's IT department configure and handle support for the network?
- How will security updates and key management occur?
- If there is a device-level security issue, who provides support?
- What are the long-term cost factors?

These are simply examples of questions to pose when selecting a wireless solution. Specific implementation location, existing wired network limitations, system connectivity, the need for mobility, and many other characteristics specific to each asset owner's environment must be evaluated.

5 Conclusions

The LOGIIC project combined research and assessment activities to reach broad conclusions about the use of wireless networking in IACS environments. Insider and outsider threat vectors were studied to create test scenarios launched during the assessment on a wireless solution that included both a WiFi and Wireless HART network. Significant research was conducted on the join process, join packet, network timing, and cryptography, including nonce and key handling.

Many facets of implementing security on a wireless network exist. This includes the join process, key handling, cryptography, and device configuration. Implementing security across these areas is needed to ensure the confidentiality, integrity, and availability required to perform control functions securely over a wireless network. If security is layered and well implemented across the wireless network, attacks will require significant resources and time.

Given the security of wireless networks and the join process, more attacks are available to simply deny connectivity rather than attacks with data change or pointed consequences. While man-in-the-middle attacks may be more difficult on a well-secured network, many threats to the wireless network exist that can create denial of service and connectivity results. These include deauthentication attacks, advertisement packet spoofing, and jamming. Jamming is perhaps the most difficult denial-of-service attack on wireless networks to prevent. Focus was placed on the recoverability of devices after jamming attacks. In many cases, devices recovered without issue. In some cases, older devices required human interaction to regain connectivity. It should be noted that during this assessment, a persistent threat is required to deny service. In this assessment, the join process and network security to protect against the outsider threat are sound. Insider threats, as expected, have a greater ability to do harm, but additional risk mitigations keep consequences minimal. Jamming attacks, as expected, are successful even with integrated security. Wireless devices recover well from jamming attacks and recover with minimal interaction after deauth attacks.

Given the fact that wireless networks can be subject to significant denial-of-service attacks as well as man-in-the- middle attacks, situational awareness is necessary to detect rogue APs and devices and general network health. Intrusion detection capabilities can be positioned to monitor for insider and outsider threats. This monitoring can provide more insight into behaviors on the network in a timely manner, instead of an operator realizing a loss of data view on a device that may only report back to the control system periodically.

Many field devices report data back to the control systems over the wireless network (e.g., control capability occurs on handheld devices for mobile operators on a plant floor). In addition to wireless network security, additional access controls and policies on the handheld devices can ensure that control functions are not exploited through easy access of distributed systems.

Like all network security methods, patching and updates are necessary to maintain a high level of security. A changing threat landscape and the increased commonality of Wireless HART requires the maintenance of strong security such as key maintenance and protection, system updates, and risk mitigation. Over time, it is expected that WiFi will continue to be an attractive target and Wireless HART may become more common. This will result in advanced attacks and toolkits available to the adversary. Asset owners must continuously maintain due diligence related to security of wireless networks based on the changing threat landscape.

The risks associated with performing control over a wireless network should be matched against the corporate operational risk profile. Considerations should include the implementation of security at all levels of the wireless network, patching and maintenance, and the structure of the network join process.

Because jamming and other denial-of-service attacks can cause non-permanent loss of control and loss of view, utilizing wireless for control functions should be considered carefully before implementation. Using wireless with control functions would likely be limited to non-critical applications that are not impacted by potential delays from jamming. Wireless is not recommended for safety functions.

Other considerations that should be made in the implementation of a wireless network in the IACS environment include:

- The return on investment calculation for a wireless network must take into account the costs associated with the resources required to design, set up, and maintain a wireless solution security.
- The development of wireless technology, to ensure that future risks are addressed and risk mitigations are provided.
- Personnel security, and ongoing training and skills upgrades to understand and maintain the protection of the most valuable elements within the wireless solution (e.g., join key).

It can be concluded that consideration of numerous factors and in-depth defenses are required to use a wireless network in the process control domain, but it is achievable with present technology. Previously mentioned limitations concerning the use of wireless solutions for critical applications must be considered.

Appendix A – Acronyms

Term/Acronym	
CSRDC	Cybersecurity Research and Development Center
DHS S&T	Department of Homeland Security Science & Technology Directorate
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
SME	Subject matter expert
Wireless HART	Wireless Highway Addressable Remote Transducer
VPN	Virtual private network