Project 5: Wireless

"Name of Presenter"

Presenter

Enter details about the presenter here.
More details about the presenter.

The LOGIIC Model of Government and Industry Partnership

Linking the Oil and Gas Industry to Improve Cyber Security

Project 5: Wireless

Background

Assessment Approach

Assessment Findings

Conclusion

Wireless

Background

Overview

- Wireless technologies monitor and control operations outside the control center
- Evaluated the security of Wi-Fi and WirelessHART
- Conducted assessments in IACS laboratory
- Findings were published in a report

Objective

- Assess wireless devices in IACS environment
- Consider vendor's ability to maintain security
- Identify important factors and risks

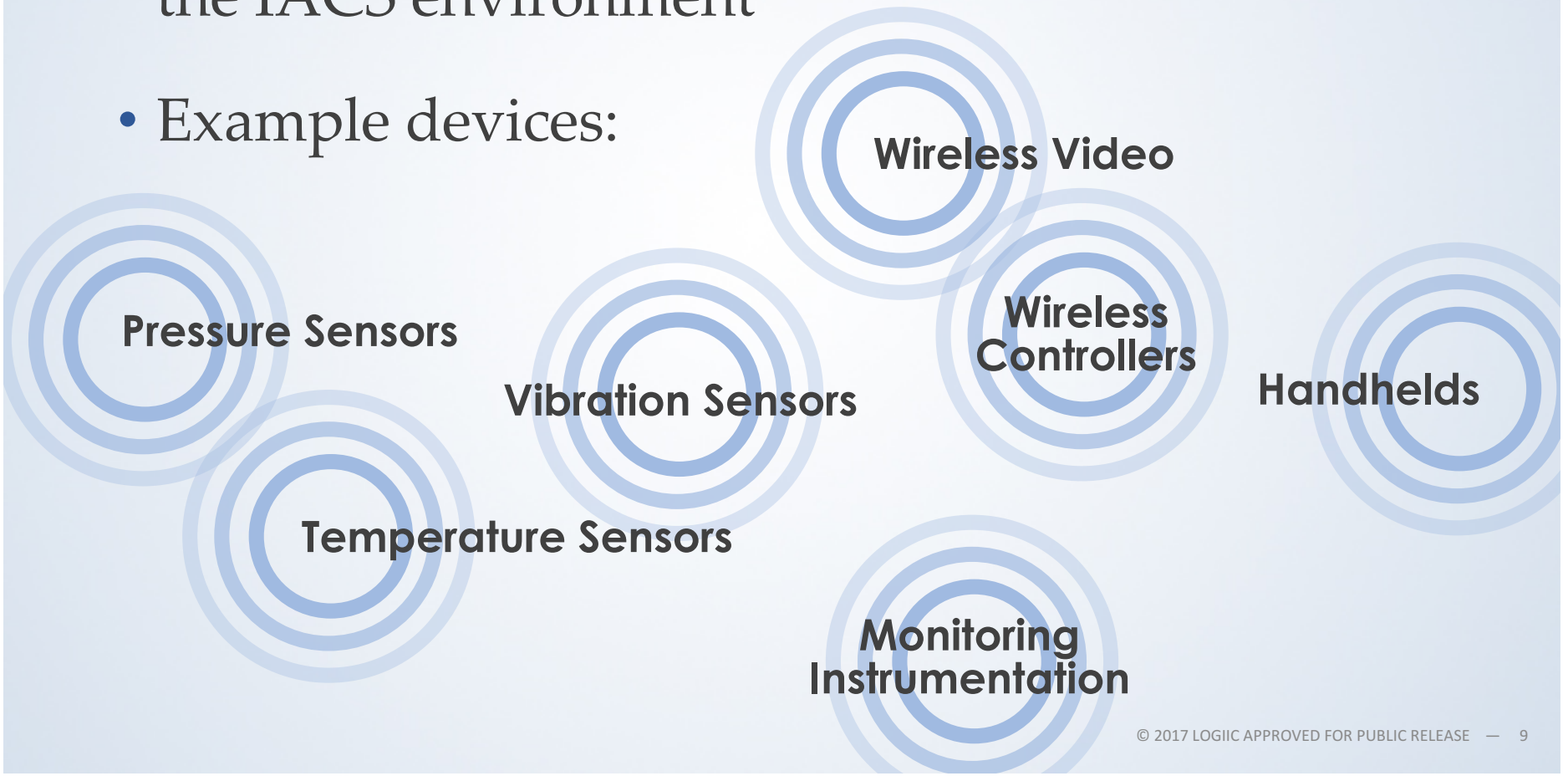
Project Approach

Test Scenarios

- Security control functionality
- Interoperability
- System availability
- Confidentiality
- Integrity

Operational Focus

- WiFi and Wireless HART devices in the IACS environment
- Example devices:



Project Considerations

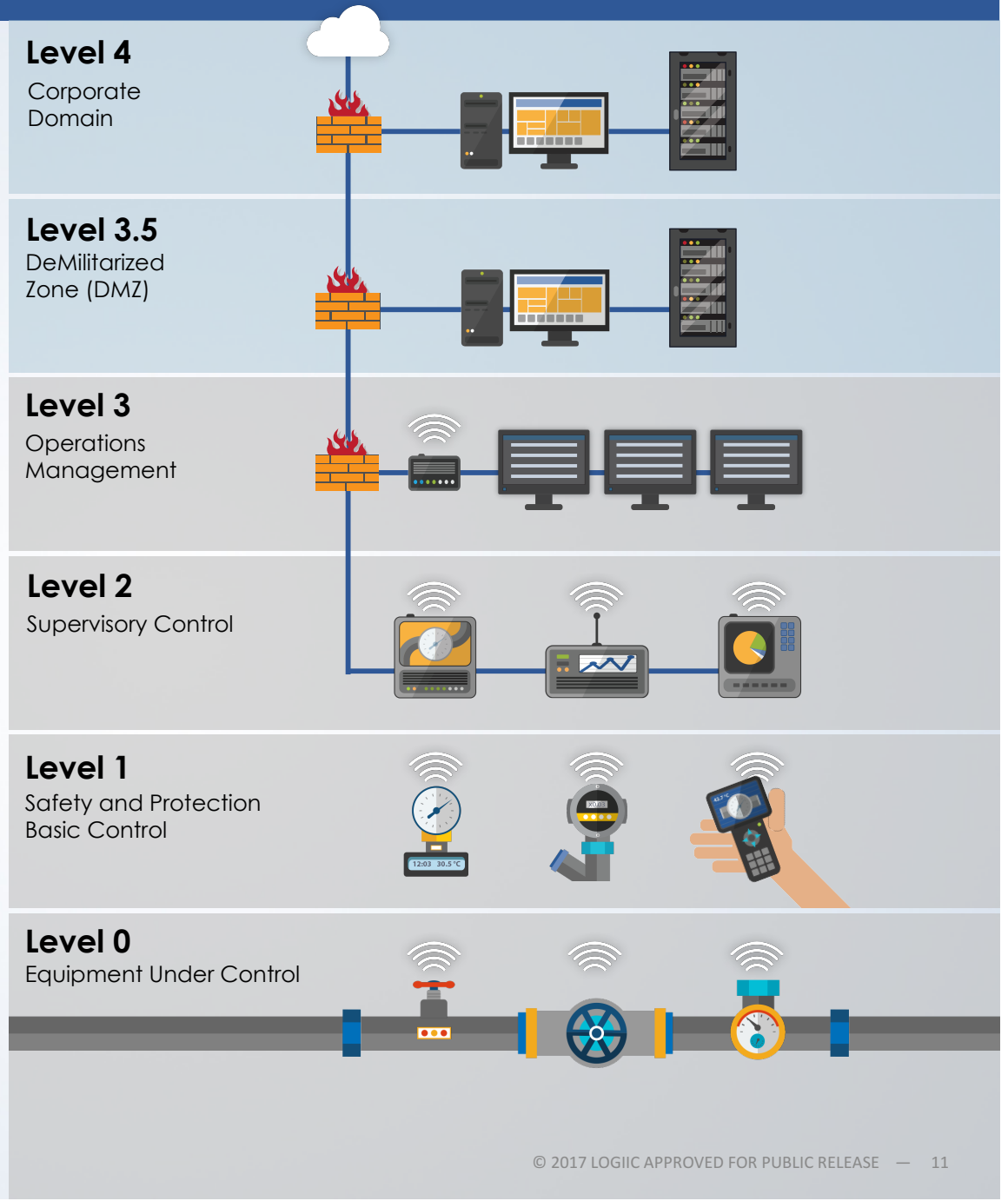
- Technical viability
- Implementation
- Maintenance
- Usability

Scope

Includes wireless technologies used with equipment and integrated systems that are part of levels 0, 1, 2, and 3 (IACS) with their extensions into 3.5 and 4.

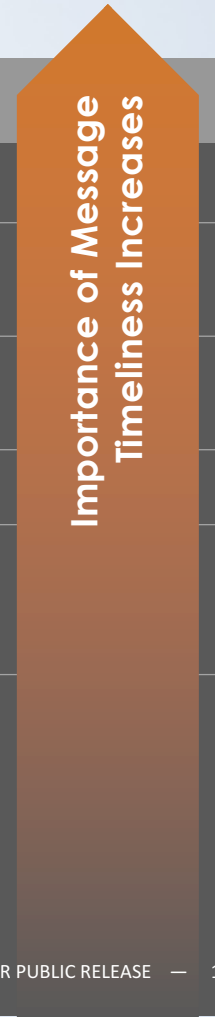
Extensions

Industrial Automation and Control Systems



Wireless solutions were considered within categories and classes of process control apps

Category	Class	Applications	Description
Safety	0	Emergency action	Always critical
Control	1	Closed loop regulatory control	Often critical
	2	Closed loop regulatory control	Usually non-critical
	3	Open loop control	Human in the loop
Monitoring	4	Alerting	Short-term operational consequences (e.g., event-based maintenance)
	5	Logging and downloading/ uploading	No immediate operational consequences (e.g, history collection, sequence-of-events, preventive maintenance)



Wireless

Assessment Approach

Methodology

Risk = Threat x Vulnerability x Consequence

Approach

Vendors + Scenarios + Rules = Plan

Onsite Assessment

- Reconnaissance
- Information capture and data retrieval attempts
- Targeted attacks
- Denial of service (DoS)

Test Approach

Insider and outsider threat scenarios

SME attack methods

Public and customized exploits and payloads

Test equipment

Test Technique Meets Objective

Technique	Confidentiality	Integrity	Availability
Packet Capture	●		
Packet Injection		●	
Session Hijacking	●	●	
Man-in-the-middle	●	●	
Packet Spoofing		●	
Packet Replay	●		
Fuzzing		●	●
Denial of Service			●
Limited Jamming			●

Pre-work

TESTING 4

TRAFFIC CAPTURE 3

NETWORK VALIDATION 2

VENDOR SET-UP 1

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

Test Scenarios

Probing

Scanning

Flooding

Connecting

Attacking

Rogue Access Points

Monitoring

Custom Scripts

Deauth

WiFi Test Tools

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





Test Scenarios

Monitoring

Packet investigstion

Rogue Gateway and Devices

Wireless HART Test Tools

Monitoring	Scanning	Probing
Wi-Analys	SCAPY	TI ZigBee Development Kits
Ubiqua	CCM* AES Utility	Awia-Tech
		Dust Networks

Analysis of Findings

TECHNICAL

Research

Documentation

Assessment Tests

Background Info

Observations

Functional Tests

OPERATIONAL

Usability

Complexity

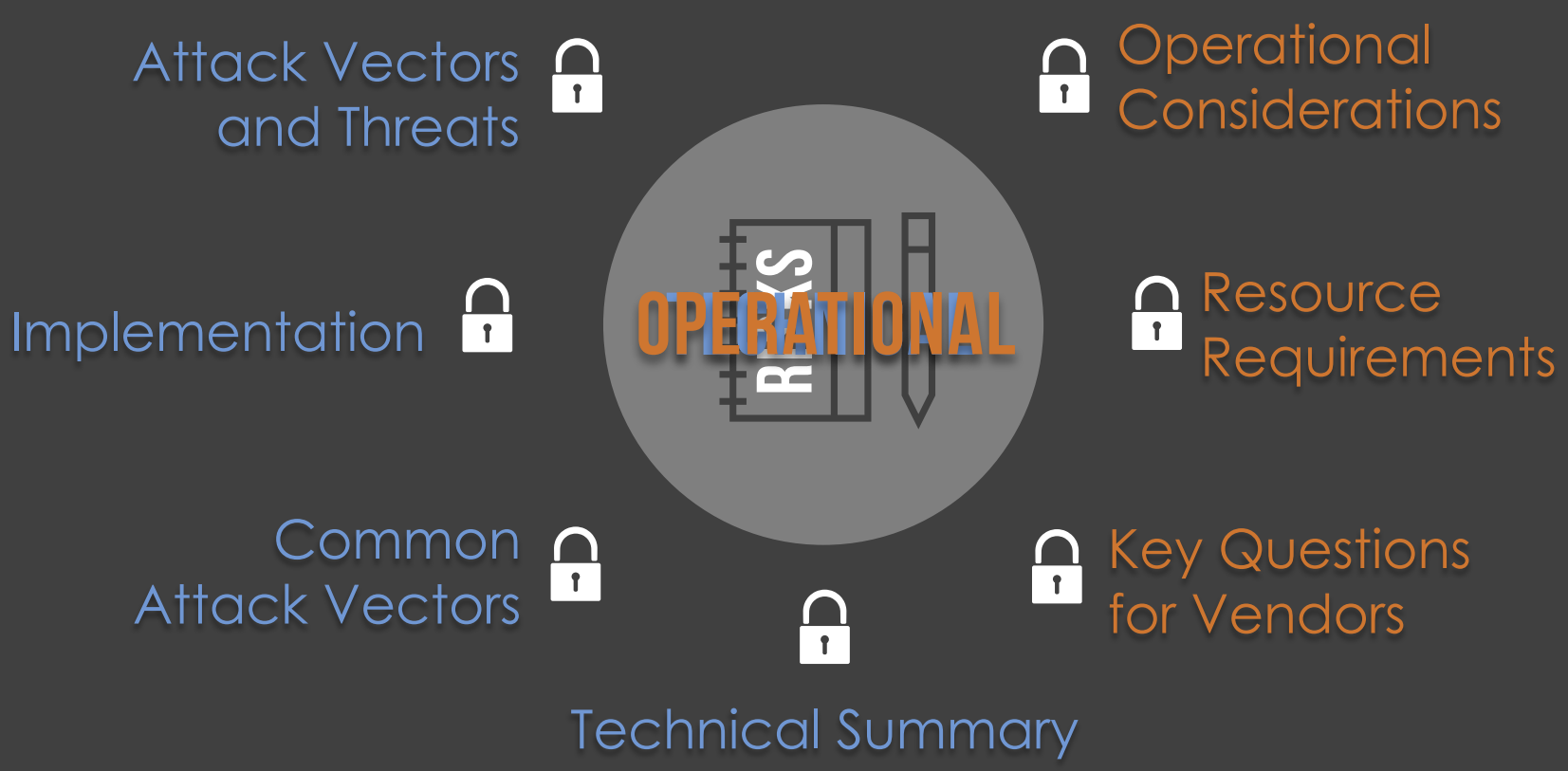
Maintenance

Connection Stability

Network
Join Times

Wireless

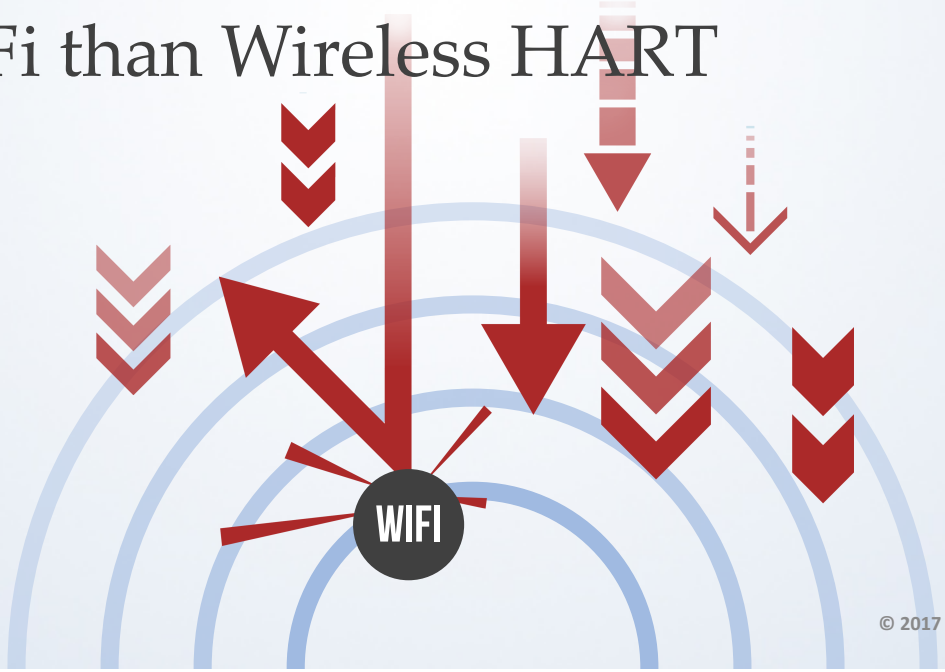
Assessment Findings


Attack Vectors and Threats
Operational Considerations
Implementation
OPERATIONAL
Resource Requirements
Common Attack Vectors
Key Questions for Vendors
Technical Summary

Wireless Attack Vectors and Threats

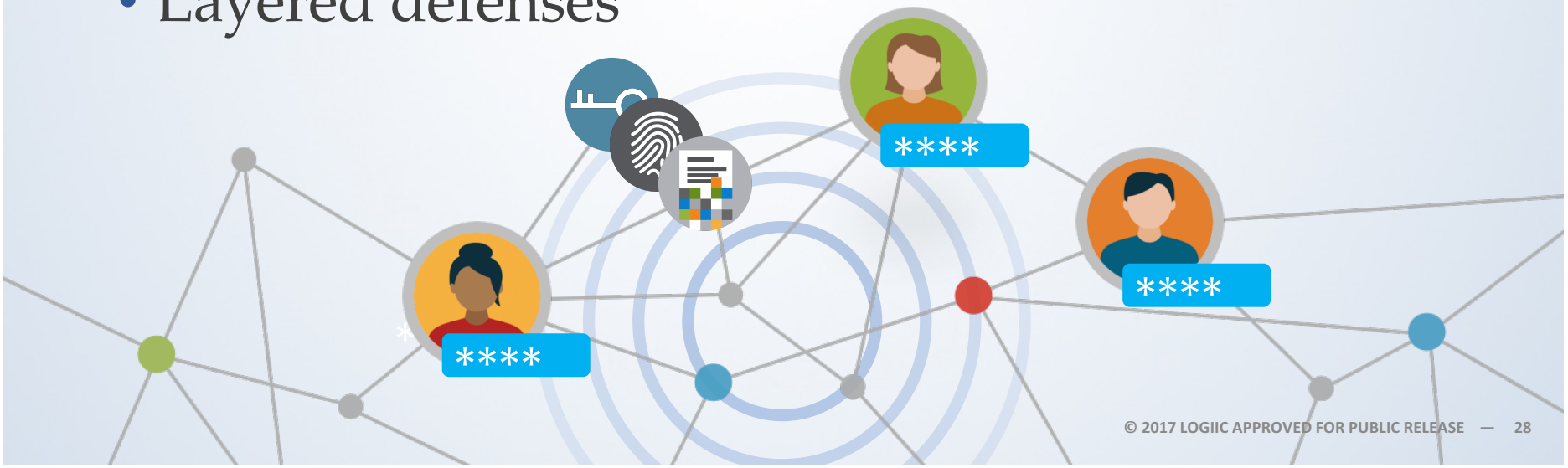
Wireless networks make attractive targets

- Insider and outsider threats
- Exploitation tools are more available with WiFi than Wireless HART



Preventing Outsider Threats

- Careful implementation of the network
- A sophisticated join and re-join process
- Successful cryptographic implementation
- Layered defenses



Preventing Insider Threats

- Layered defenses
- Role-based access control
- Physical security

Denial of Service

- A reality for any wireless network, particularly jamming
- Requires less reconnaissance, fewer resources
- Difficult to prevent, but networks can recover

- DoS attacks in this project included:
  - Deauth attacks
  - Jamming
  - Network flooding
  - Fuzzing
- Persistent threats utilize resources and risk identification

Man-in-the-Middle

- Requires outsider penetration of the network or insider access to the network
  - Sophisticated tools
  - Understanding of the network
  - Exploitable vulnerability

- Exploiting Wireless HART
  - Highly complex and resource-intensive
  - Tools not readily available

Implementation Considerations

Several elements should be addressed to ensure security of the entire network

Network Join Process

- Prevention requires:
  - Network & session keys
  - Join key rotation
  - Key structure
  - Key protection
  - Key use policies
- Critical to overall network security
- Owners must evaluate prior to implementation

Cryptographic Attributes

- Careful implementation of cryptography throughout join and rejoin process

- Successful attacks through packet injection would be extremely resource intensive

Example:
Nonce Process

Network Resilience

- Vulnerable to denial of service and connectivity
- Recoverability and the rejoin process must be sound and tested to ensure viability

Common Attack Vectors

Readily available tools, custom scripting, and common exploits were used to assess and understand impact of the following common attack vectors.

Ad Packet Spoofing

- Bombardment of false ads can prevent a device from connecting to a valid network, which was validated during testing
- A persistent threat is continually bombarded

Rogue Access Points

- Easily prevented with layered security
- Security from the join process and cryptography prevented rogue access points during testing

Fuzzing

- Directed flooding of specific packets
- Requires significant resources to be successful
- Well-implemented security can prevent fuzzing

Jamming

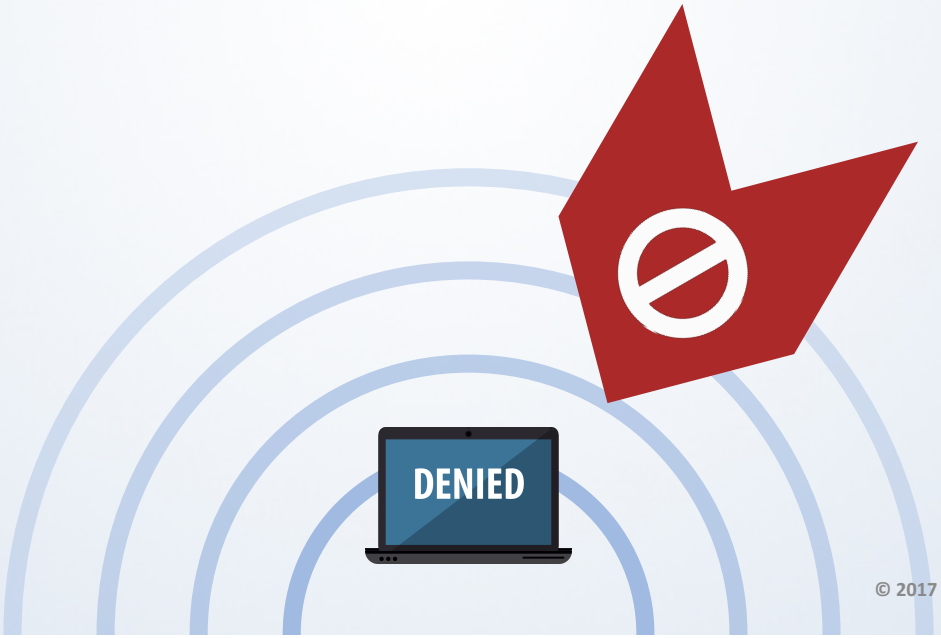
- All wireless devices are susceptible to jamming
- Recoverability: immediate vs interaction
- Some devices required reboot or reset

- Can simply make a device appear out of range
- Jamming at a distance likely affects systems in very close proximity in the same way

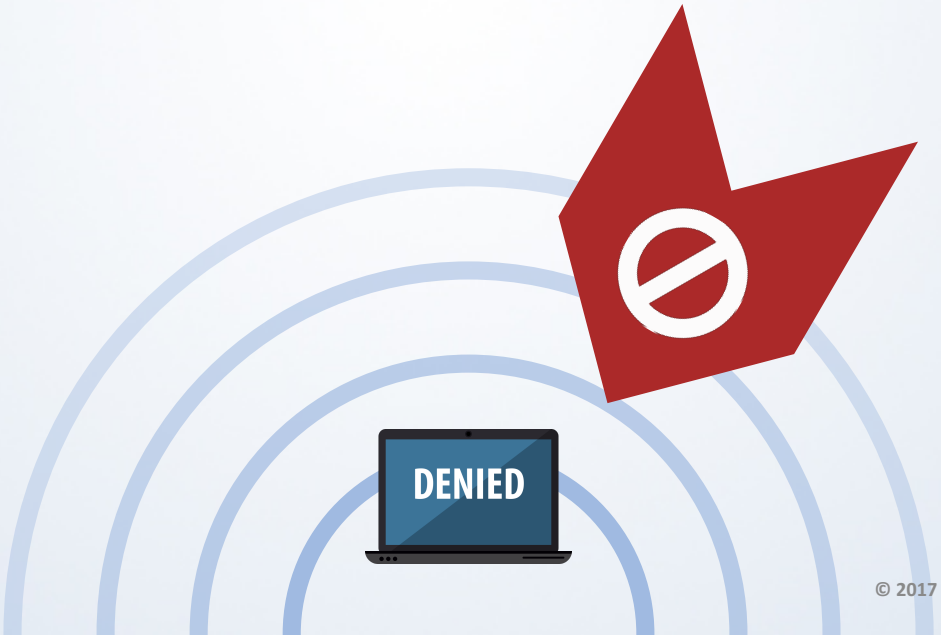
- Difficult to distinguish jamming from other network problems
- A large RF was required to jam a controller
- Wireless HART devices may be easier targets due to low power output

Deauth Attacks

- Deauthentication attacks use well known tools to deny access to specific devices
- Successfully denied connectivity to WiFi devices, resulting in loss of data view



- When deauth attacks stop, some devices recover, other require diagnostics or a reboot
- Can be successful DoS attacks requiring interaction to recover functionality



Summary of Technical Findings

Technical Findings	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
Ad Packet Spoofing	Affected	Not Affected	Not Affected
Wireless HART Nonce	Not Affected	Not Affected 2	Not Affected 2
Wireless HART Packet	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

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

Operational Considerations

Asset owners are encouraged to discuss these considerations with their automation vendor when selecting and implementing a wireless solution.

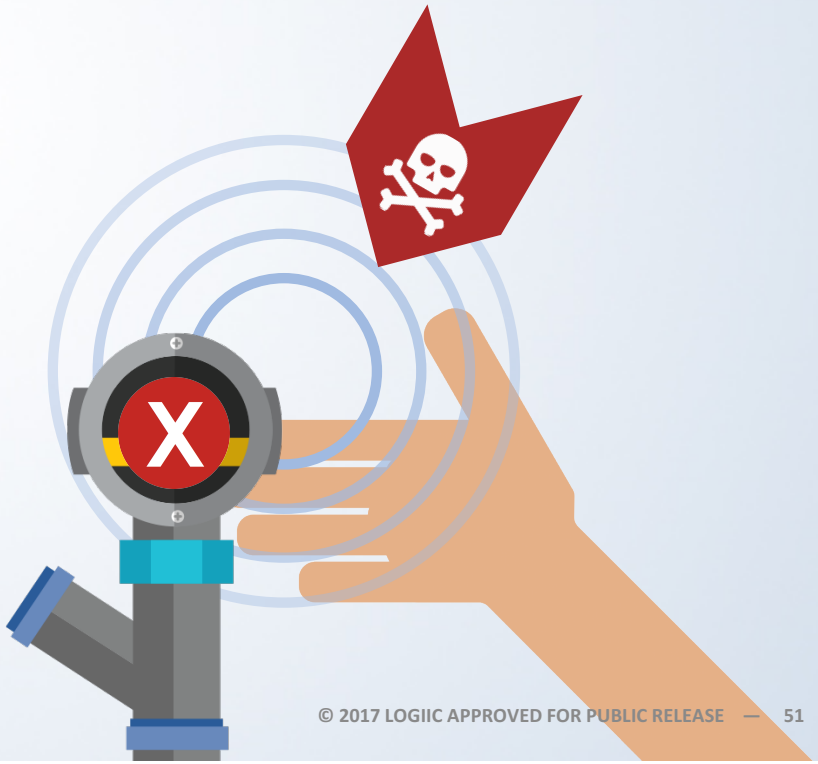
- Setup less time consuming
- Impenetrable from outsider threats
- Specific attacks more complex

- Setup more time consuming and resource intensive
- Impenetrable from outsider threats
- More tools exist to target WiFi

Intrusion Detection and Monitoring

- Because DoS and loss of connectivity are common threats, situational awareness is important
- Devices may only provide data intermittently, therefore views on the operator console may be uninformative

- Network attacks can be difficult to distinguish
- Intrusion detection may identify rogue access points, network health, or other threats before an operator realizes devices have lost connectivity



Supply Chain Viability

- Owners conducting controls need full clarity of security mechanisms, components, and solution
- Solutions from mixed device manufacturers require vendors assurance:
  - Comprehensive security
  - Documentation of the join process and security layers
  - Solution meets export control guidelines

Control Isolation

- Reachback to control systems from the wireless network must be protected
- Integrity of field device data must be ensured
- VPNs, layered access control, and firewalls

Handheld Devices for Mobile Operators

- Might perform control functions
- Consider role-based access control, physical security, and use policies
- Significant insider threats
  - left unattended
  - user log-out
  - screen lock

Resource Requirements

Prior to selection, asset owners should consider:

- Architectures
- Risk portfolio
- Maintenance

Key Questions for Vendors

- 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?

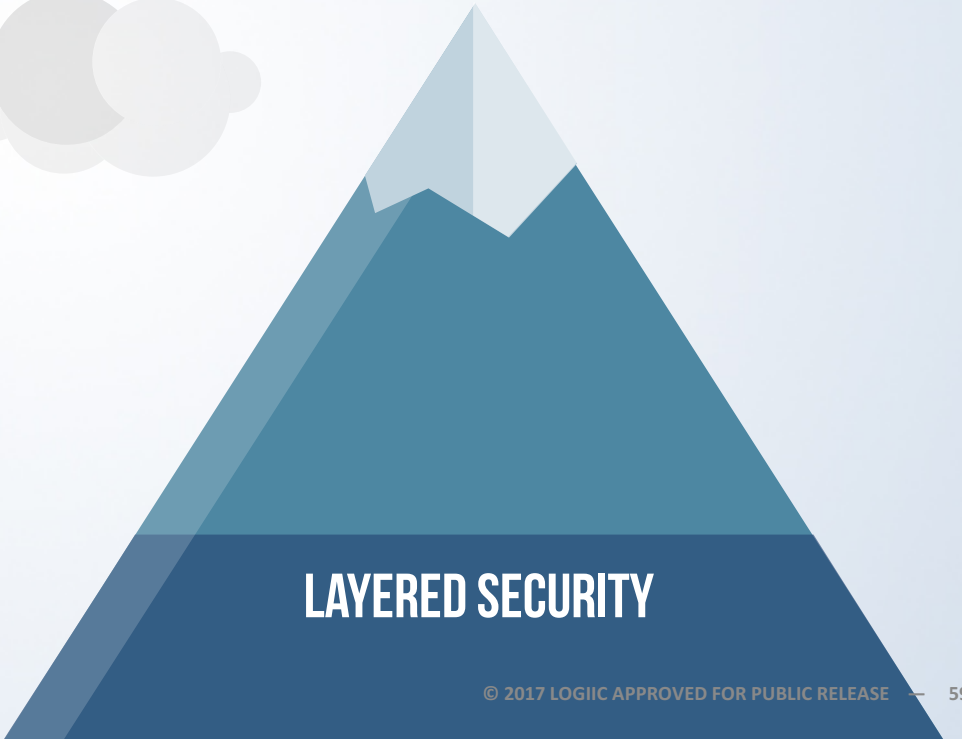
- How will security updates and key management occur?
- If there is a device-level security issue, who provides support?
- What are the long-term cost factors?

Wireless

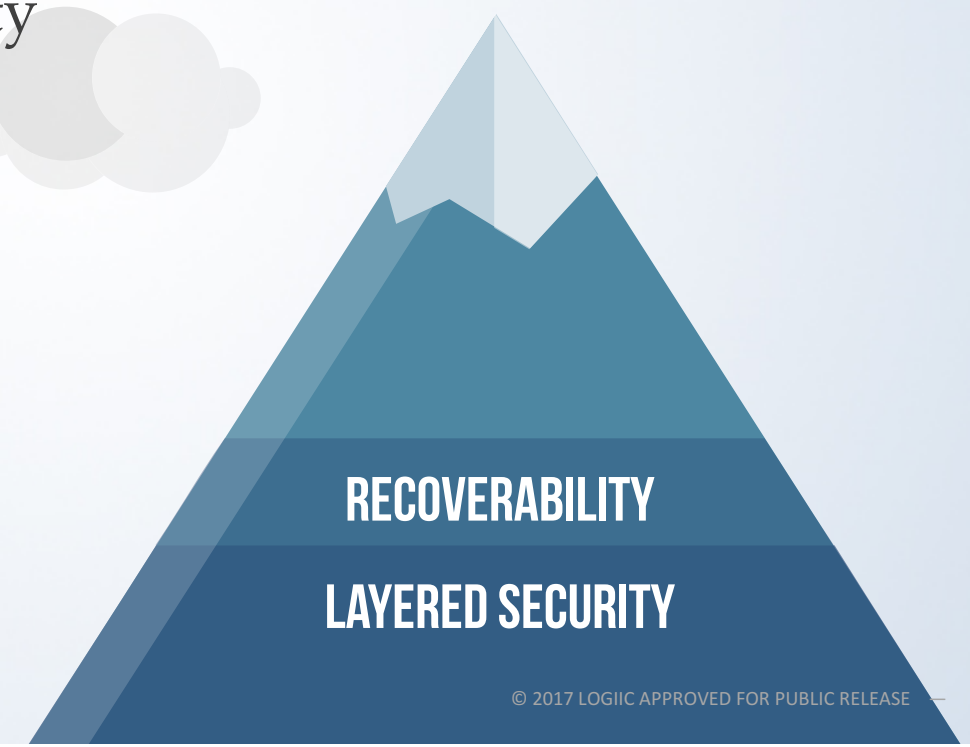
Conclusion

Conclusions

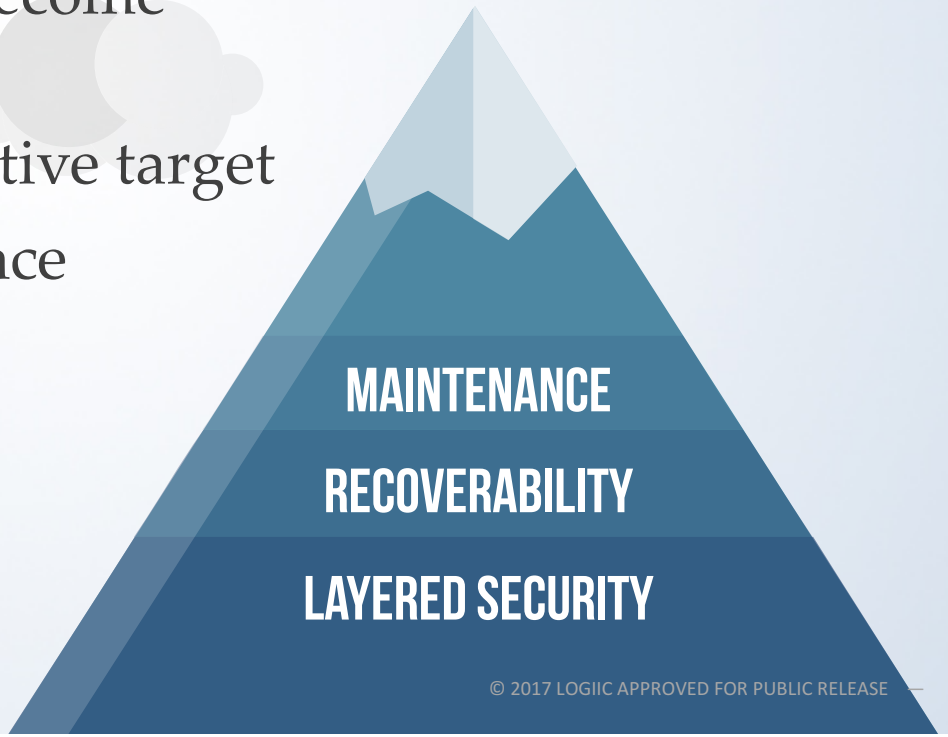
- Many facets of implementation
  - Network join process
  - Key handling
  - Cryptography
  - Device configuration
- Layered security challenges the threat



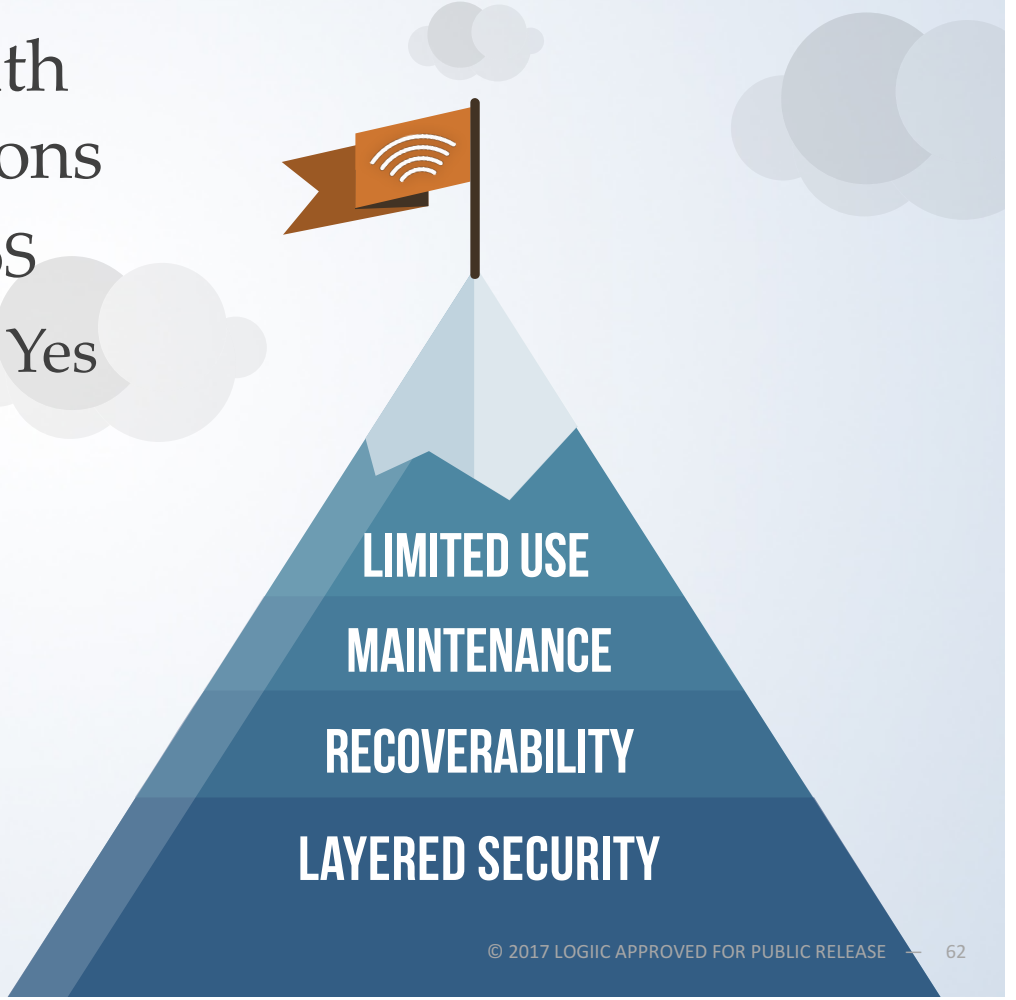
- More attacks deny connectivity rather than alter data
  - Deauth, ad spoofing, and jamming
- Jamming is most difficult to prevent
  - Focus on recoverability
- Monitoring can help
  - Rogue access points
  - Jamming



- Key maintenance and protection, system updates, and ongoing risk mitigation
- Changing threat landscape
  - Wireless HART may become an attractive target
  - WiFi remains an attractive target
  - Continuous maintenance



- Performance control risks vs. corporate operational risks
- Limit wireless use with facility control functions
  - Jamming and other DoS
  - Non-critical functions: Yes
  - Safety functions: No



Additional Considerations

- Return on investment for design, setup, and maintenance of security
- Development of wireless technology and mitigation of emerging risks
- Personnel security, training, and skills to maintain security of the wireless solution

Numerous factors and
in-depth defenses are required
to use a wireless network
in a process control domain,
but it is achievable
with present technology.