Wireless in OT Environments

WiFi, 5G, LoRaWAN, and industrial wireless security

OT Security Learning Series

Document 305 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Wireless technologies are increasingly deployed in OT environments for mobility, flexibility, and cost reduction. However, they introduce unique security challenges that differ significantly from wired networks.

Common wireless use cases in OT:

- Mobile HMI and tablets for operators
- Wireless sensor networks
- Remote asset monitoring (IoT/IIoT)
- Temporary connections during maintenance
- Connectivity in hazardous or hard-to-wire areas

Warning

Wireless extends the attack surface beyond the physical perimeter. An attacker doesn't need physical access—they only need to be within radio range.

2 Wireless Technologies in OT

2.1 Technology Comparison

Technology	Range	Speed	OT Use Case
WiFi (802.11)	50–100m	High	HMI, video, general data
5G / LTE	1–10km	High	Remote sites, mobile assets
LoRaWAN	2–15km	Low	Sensors, metering
WirelessHART	50–250m	Low	Process instrumentation
ISA100.11a	50–250m	Low	Process automation
Zigbee	10–100m	Low	Building automation
Bluetooth	10–100m	Medium	Local device pairing

Table 1: Wireless Technologies Comparison

2.2 Industrial Wireless Standards

Industrial Wireless Protocols

- **WirelessHART** – Extension of HART protocol for process control
- **ISA100.11a** – ISA standard for industrial automation
- **WiFi (802.11)** – General purpose, widely deployed
- **5G/Private LTE** – High bandwidth, low latency, wide area

3 Security Risks

3.1 Wireless-Specific Threats

Threat	Description
Eavesdropping	Passive interception of wireless traffic
Rogue Access Points	Unauthorized APs capturing credentials
Evil Twin	Fake AP mimicking legitimate network
Deauthentication	Forcing clients to disconnect (DoS)
Man-in-the-Middle	Intercepting and modifying communications
Jamming	Radio interference causing denial of service
Wardriving	Scanning for vulnerable wireless networks
Credential Theft	Capturing authentication handshakes

Table 2: Wireless Security Threats

3.2 OT-Specific Concerns

Critical

Critical OT wireless risks:

- Safety system commands over wireless
- Unencrypted legacy industrial protocols
- Interference with control system timing
- Extended attack surface beyond fence line
- Difficulty detecting rogue devices

4 WiFi Security

4.1 WiFi Security Standards

Standard	Encryption	Recommendation
WEP	RC4 (broken)	Never use
WPA	TKIP	Avoid
WPA2-Personal	AES-CCMP	Acceptable for low-risk
WPA2-Enterprise	AES + 802.1X	Recommended
WPA3	SAE + AES-GCM	Best available

Table 3: WiFi Security Standards

4.2 WiFi Best Practices

Key Point

Minimum requirements for OT WiFi:

- WPA2-Enterprise or WPA3
- 802.1X authentication with RADIUS
- Dedicated SSIDs for OT (separate from corporate)
- Certificate-based authentication where possible
- Wireless IDS/IPS deployment

- Disable SSID broadcast (limited value but reduces casual discovery)
- Use strong, unique passwords (if PSK required)
- Enable client isolation where appropriate
- Implement MAC filtering as additional layer
- Regular wireless surveys to detect rogues
- Position APs to minimize signal leakage outside facility

5 5G and Private LTE

5.1 Benefits for OT

- **Private networks** – Dedicated spectrum, full control
- **Low latency** – Suitable for real-time control
- **High reliability** – Carrier-grade availability
- **Wide coverage** – Large facilities, remote sites
- **Built-in security** – SIM-based authentication

5.2 5G Security Considerations

- Use private 5G networks, not public carriers for critical systems
- Implement network slicing for traffic isolation
- Secure the 5G core infrastructure
- Monitor for IMSI catchers and fake base stations
- Encrypt application layer (don't rely only on 5G encryption)

6 LPWAN (LoRaWAN, NB-IoT)

6.1 Low-Power Wide-Area Networks

Common for remote sensors and metering:

- **LoRaWAN** – Long range, low power, open standard
- **NB-IoT** – Cellular-based, carrier managed
- **Sigfox** – Ultra-narrow band, limited messages

6.2 LPWAN Security

Warning

Many LPWAN deployments use default keys or weak security. Always:

- Change default application and network keys
- Use unique keys per device
- Enable encryption (LoRaWAN AES-128)
- Implement secure join procedures (OTAA over ABP)

7 Implementation Guidelines

7.1 OT Wireless Architecture

1. **Segment** – Separate SSID/VLAN for OT wireless
2. **Firewall** – All wireless traffic through OT firewall
3. **Authenticate** – 802.1X, certificates, or strong PSK
4. **Encrypt** – WPA2-Enterprise minimum, WPA3 preferred
5. **Monitor** – Wireless IDS, rogue AP detection
6. **Limit** – Restrict wireless to non-safety applications

7.2 What NOT to Put on Wireless

Critical

Avoid wireless for:

- Safety Instrumented Systems (SIS)
- Emergency shutdown commands
- Primary control loops
- High-speed motion control
- Any application where latency/jitter is critical

8 Monitoring and Detection

- Deploy Wireless Intrusion Detection Systems (WIDS)
- Conduct regular wireless site surveys
- Monitor for unauthorized SSIDs and clients
- Alert on deauthentication floods
- Track RF spectrum for jamming attempts
- Maintain inventory of authorized wireless devices

9 Summary

Key Takeaways

- **Extended attack surface** – Wireless reaches beyond physical perimeter
- **WPA2-Enterprise minimum** – No WEP, no WPA-Personal in OT
- **Segment OT wireless** – Separate from corporate networks
- **Monitor continuously** – Rogue AP and intrusion detection
- **Avoid for safety** – Don't use wireless for safety-critical functions
- **Industrial protocols** – WirelessHART, ISA100.11a for process control

10 Further Reading

Standards

- **IEC 62443-3-3** – Wireless security requirements
  https://webstore.iec.ch/publication/7033

- **ISA-TR100.15.01** – Wireless backhaul recommendation
  https://www.isa.org/

Resources

- **NIST SP 800-153** – Guidelines for Securing WLAN
  https://csrc.nist.gov/publications/detail/sp/800-153/final
- **CISA – Wireless Security**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series