Security of Wireless Sensors & Networks at PERA Level 0 to 1

MLM-079-A

Industry – All
Principal Role – All
Professional Role – Control Engineers
Enterprise Phase – Design &Operation

Turn on your audio and click start to begin video

START

This MLM examines the reliability and cybersecurity of commonly used wireless industrial networks.

Click the NEXT button when you are ready to advance to the next slide.

Wireless Protocols for Plant Instrumentation

The following are two of the most common wireless networks for industrial applications (e.g., a continuous chemical process or a batch pharmaceuticals facility).

- Wireless Hart
- ISA 100.11a

Other common wireless sensor networks include Zigbee, Thread, and Z-wave. These are also low power, multi-path radio networks that share many characteristics of Wireless Hart and ISA 100 so we will not specifically address them in this module.

For discrete manufacturing (e.g., automotive industry there are many others, but these will not be discussed in this Module).

2

The following are two of the most common wireless networks for industrial applications (e.g., a continuous chemical process or a batch pharmaceuticals facility).
Wireless Hart
ISA 100.11a

Other common wireless sensor networks include Zigbee, Thread, and Z-wave. These are also low power, multi-path radio networks that share many characteristics of Wireless Hart and ISA 100 so we will not specifically address them in this module.

For discrete manufacturing (e.g., automotive industry there are many others, but these will not be discussed in this Module).

Commercial Offerings

- More than 200 instrumentation companies offer Wireless LAN products including:

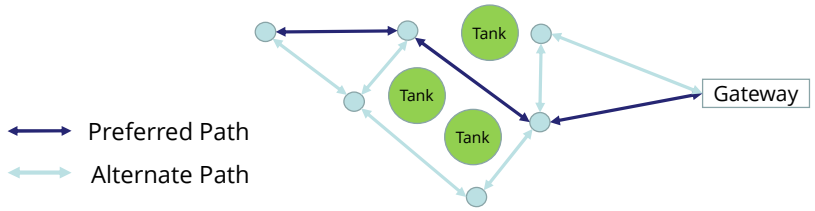
3

More than 200 instrumentation companies offer Wireless LAN products, including ABB, Emerson, Honeywell, Siemens and Yokogawa.

Comparison of Wireless Hart and ISA 100.11a

Similarities

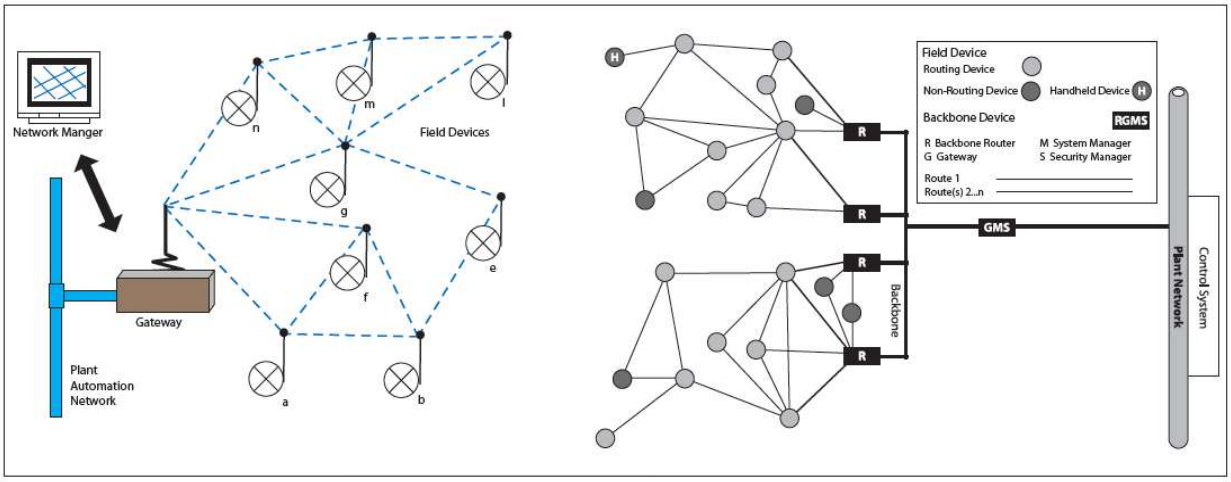
- Both use the same low power IEEE 802.15.4 radio (same range, beam propagation patterns). Both are often battery powered.
- Both are mature technology that has been in use for over 10 years.
- "Mesh networking" overcome range and obstruction problems.
- Dynamic "Self-healing" bypasses device failures or wave-path obstructions.



4

Similarities include:
Both use the same low-power IEEE 802.15.4 radio (same range, beam propagation patterns). Both are often battery-powered.
Both are mature technologies that have been in use for over 10 years.
"Mesh networking" overcomes range and obstruction problems.
Dynamic "Self-healing" bypasses device failures or wave-path obstructions.

Comparison of Wireless Hart and ISA 100.11a (cont'd)



Wireless HART has no backbone

ISA100.11a defines a high speed backbone

Comparison of Wireless Hart and ISA 100.11a (cont'd)

Wireless Hart

- "Self-organizing" is much easier to configure and deploy.
- However, inability to over-ride automatic configuration may result in:
  - bandwidth bottlenecks,
  - common points of failure may shut down large areas
- Dynamic re-configuration results in "attack surfaces" for cyber intruders (eg., "worm-hole exploit").
- Lack of monitoring tools makes optimization, network performance and security monitoring difficult or impossible.
- Only 100 nodes can be configured per Gateway, and performance issues often limit this further.

6

Wireless Hart is

- "Self-organizing,"so it is much easier to configure and deploy.
- However, the inability to override automatic configuration may result in:
  - bandwidth bottlenecks,
  - common points of failure may shut down large areas
- Dynamic re-configuration results in "attack surfaces" for cyber intruders (e.g., "worm-hole exploit").
- Lack of monitoring tools makes optimization, network performance, and security monitoring difficult or impossible.
- Only 100 nodes can be configured per Gateway, and performance issues often limit this further.

Comparison of Wireless Hart and ISA 100.11a (cont'd)

ISA 100.11a

- **"User configured," so the design requires more expertise and time.**
- **Configuration tools allow:**
  - Optimization of Network Paths and backup configuration (e.g., pinch-points)
  - Monitoring of Network bandwidth and reconfiguration as needed
  - Configuration of "mesh" where needed, but can also define primary and backup paths.
  - Larger networks with multiple gateways and routers.
  - Detection of unexpected traffic (e.g., cyber attacker).

ISA 100.11a is:

- "User configured," so the design requires more expertise and time.
- Configuration tools allow:
  - Optimization of Network Paths and backup configuration (e.g., pinch-points)
  - Monitoring of Network bandwidth and reconfiguration as needed
  - Configuration of "mesh" where needed but can also define primary and backup paths.
  - Larger networks with multiple gateways and routers.
  - Detection of unexpected traffic (e.g., cyber attacker).

Battery Life is a Reliability Consideration

Eliminating signal & power wiring is a key Wireless benefit, however:

- If a network includes Analyzers (like Gas Chromatographs) or slow measurements like tank levels, radio transmitters need only "awaken" every couple of minutes, and battery life may be a couple of years.
- but, if a network includes safety gas sensors or high-speed sensors or analyzers used for control, it may be necessary to poll these devices every second. In this case, that same battery could be exhausted in a week. (365x2/60x2 = ~7 days)
- Even worse, in a self-configuring network, adding a device that is polled every few seconds, could suddenly exhaust the batteries of devices that only "pass on" the data in a mesh network.

Batteries are improving – New technology is significantly extending battery life and changing batteries in hazardous areas is getting easier and safer.

Solar Panels have dropped in price dramatically, so may work in some networks.

8

Eliminating signal & power wiring is a key Wireless benefit, however:

- If a network includes Analyzers (like Gas Chromatographs) or slow measurements like tank levels, radio transmitters need only "awaken" every couple of minutes, and battery life may be a couple of years.
- but, if a network includes safety gas sensors or high-speed sensors or analyzers used for control, it may be necessary to poll these devices every second. In this case, that same battery could be exhausted in a week. (365x2/60x2 = ~7 days)
- Even worse, in a self-configuring network, adding a device that is polled every few seconds could suddenly exhaust the batteries of devices that only "pass on" the data in a mesh network.

Batteries are improving – New technology is significantly extending battery life, and changing batteries in hazardous areas is getting easier and safer.

Solar Panels have dropped in price dramatically, so they may work in some networks.

Management of Change

- Connecting a device to an industrial network (wired or wireless) requires special equipment, procedures & training.
- Adding new network types or replacing old ones requires a large investment of manpower and equipment.
- If existing networks are to be changed, it must therefore be for well-considered reasons and be carefully planned and funded.

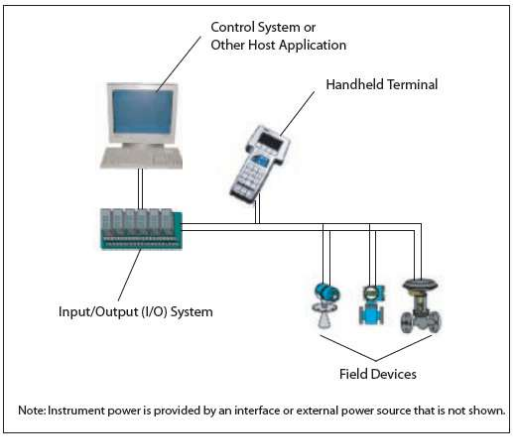


Figure 2. Typical HART system (courtesy of HCF)

9

Connecting a device to an industrial network (wired or wireless) requires special equipment, procedures & training.

Adding new network types or replacing old ones require a large investment of manpower and equipment.

If existing networks are to be changed, it must therefore be for well considered reasons and be carefully planned and funded.

Management of Change (cont'd)

Network Configuration Management is essential to:

- Ensure approval and documentation of network changes
- Protect updates and "patches" (Solar Wind Hack)
- Test network configurations (using simulation tools)
- Monitor bandwidth problems and failure modes
- Detect and isolate suspicious network traffic (may not be able to stop penetration, but must know they are there)
- See ISA 108 Intelligent Device Configuration and Management

10

Network Configuration Management is essential to:

- Ensure approval and documentation of network changes
- Protect updates and "patches" (Solar Wind Hack)
- Test network configurations (using simulation tools)
- Monitor bandwidth problems and failure modes
- Detect and isolate suspicious network traffic (may not be able to stop penetration, but must know they are there)
- See ISA 108 Intelligent Device Configuration and Management

New Wireless Alternatives

- **LoRaWAN** – Low Power High Bandwidth Wide Area Network.
- **WiFi** – Industrial "hardened" versions of popular commercial LAN.
- **5G** – 5th Generation "microwave broadband"

Some key features of these are discussed below.

LoRaWAN – Low Power High Bandwidth Wide Area Network.

WiFi – Industrial "hardened" versions of popular commercial LAN.

5G – 5th Generation "microwave broadband"

Some key features of these are discussed below.

New Wireless Alternatives (cont'd)

Low power Radio Wide Area Network (LoRaWAN)

- Low power, high bandwidth based on "chirp" spread-spectrum tech.
- Range of several miles (depending on terrain and obstacles)
- Easy attachment of IoT and IIoT devices (local, regional and global).
- Provides end-to-end security (frequency agile spread-spectrum was invented for torpedoes).
- Scalable to very Large Networks
- Supports "cloud" connections
- Sophisticated configuration, optimization and monitoring tools
- Subject to jamming, spoofing and other radio network vulnerabilities

12

Low power Radio Wide Area Network (LoRaWAN)
Low power, high bandwidth based on "chirp" spread-spectrum tech.
Range of several miles (depending on terrain and obstacles)
Easy attachment of IoT and IIoT devices (local, regional and global).
Provides end-to-end security (frequency agile spread-spectrum was invented for torpedoes).
Scalable to very Large Networks
Supports "cloud" connections
Sophisticated configuration, optimization and monitoring tools
Subject to jamming, spoofing, and other radio network vulnerabilities.

New Wireless Alternatives (cont'd)

Industrial version of commercial Wi-Fi Network

- Many suppliers of low-cost, reliable chips and components
- Supports mesh networking, self-healing, and multi-layer IP routing
- Sophisticated Network configuration and Monitoring Tools
- Most Technicians already know how to configure and troubleshoot
- Well integrated in all common operating systems
- Easily integrated with other networks, including Ethernet, 5G, etc.
- Unlike a cellular network, Wi-Fi can be configured with different levels of security. WPA2-Enterprise options are accepted for secure, secret government and military networks.

Industrial version of commercial WiFi Network

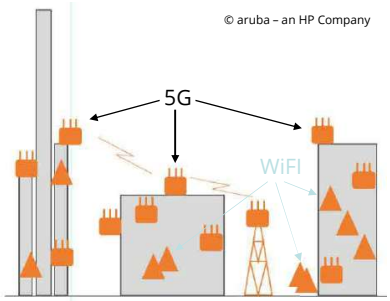
- Many suppliers of low-cost reliable chips and components
- Supports mesh networking, self-healing, and multi-layer IP routing
- Sophisticated Network configuration and Monitoring Tools
- Most Technicians already know how to configure and troubleshoot
- Well integrated in all common operating systems
- Easily integrated with other networks including Ethernet, 5G, etc.
- Unlike a cellular network, Wi-Fi can be configured with different levels of security. WPA2-enterprise options are accepted for secure and secret government and military networks.

New Wireless Alternatives (cont'd)

5th Generation Private and Public Networks

- Special frequencies are reserved for private "campus networks"
- Time Critical Network standards are in testing.
- Easily integrated with other networks, including Ethernet, Wi-Fi, etc.
- Highly scalable (to city or even nation-wide networks).

- Configure Wi-Fi inside structures
- Use 5G for "outside" networks
- Consistent "top to bottom"
  - Authentication and encryption
  - Configuration
  - Monitoring and optimization
  - Cyber defense and response



14

5th Generation Private and Public Networks provide new wireless alternatives such as:

- Special frequencies are reserved for private "campus networks"
- Time Critical Network standards are in testing.
- Easily integrated with other networks, including Ethernet, Wi-Fi, etc.
- Highly scalable (to city or even nation-wide networks).

They may be Configured as
- Wi-Fi inside structures
- Use 5G for "outside" networks

Consistent "top to bottom"
- Authentication and encryption
- Configuration
- Monitoring and optimization
- Cyber defense and response

Cybersecurity and Reliability of Wireless Networks

- **<u>Legacy radio networks</u> are less cybersecure and reliable than wired networks because of:**
  - Inherent "attack surfaces" (e.g. worm-hole)
  - Small user base
  - Battery failures
  - Weaker configuration and monitoring tools

Legacy radio networks are less cybersecure and reliable than wired networks because of:

- Inherent "attack surfaces" (e.g. worm-hole)
- Small user base
- Battery failures
- Weaker configuration and monitoring tools

Cybersecurity and Reliability of Wireless Networks (cont'd)

- **New Radio networks like LoRaWAN, WiFi and 5G can be more cybersecure than traditional wireless and wired networks because:**
  - Better monitoring tools detect bandwidth problems and misconfiguration
  - Wider user base detects vulnerabilities and eliminates bugs.
  - Better configuration management detects unauthorized changes (whether poor practices or cyber attacks).
  - Artificial intelligence monitoring can detect anomalous traffic (more sophisticated protocols - Blackberry example)

16

New Radio networks like LoRaWAN, WiFi and 5G can be more cybersecure than wired networks because:
- Better monitoring tools detect bandwidth problems and misconfiguration
- Wider user base detects vulnerabilities and eliminates bugs.
- Better configuration management detects unauthorized changes (whether poor practices or cyber attacks).
- Artificial intelligence monitoring can detect anomalous traffic (more sophisticated protocols - Blackberry example)

Author

Gary has more than 40 years of experience with enterprise integration and optimization projects, including PERA master planning and project management.

As one of the initial authors of the PERA Handbook of Master Planning, he has used PERA Enterprise Architecture and Master Planning methodologies throughout his career including control and information systems for oil production, pipelines, refining and marine loading, petrochemicals, coal, gas, and oil-fired power plants, polyethylene, ammonia, explosives, paint, pulp and paper, food and beverage, and pharmaceuticals. LNG facilities included world-scale Arctic, European, and US Gulf Coast complexes.

infrastructure facilities included Fire, Police, and Emergency Response systems for major US cities, as well as emissions reporting and trading systems for more than 100 US Power Plants.

Please click here to provide feedback on this MLM.