PlantWeb University – Wireless 403

Planning and Installation of Self-organizing Networks

25 minutes

In this course:

Overview

Self-organizing networks are a promising wireless solution for the process industry – in part because they're so easy to plan, commission, and install.

All wireless field networks are easier and less costly to install than traditional wired systems, simply because they're wireless. They use radio signals to carry messages from the wireless field devices to the gateway, so there's no expensive cabling to install.

But unlike other wireless field network solutions – such as line-of-sight or point-to-point networks – self-organizing networks don’t require detailed site surveys or specialized equipment to implement. They're also much easier to expand.

Although many aspects of installing a self-organizing network are similar to procedures you probably already use for wired networks, there are some differences. A self-organizing network is an entire system of interconnected communications, so all the components have to work together. Planning – in advance, and for the future – is key to a successful implementation.

In this course you’ll learn the basic steps for easy planning and installation of a robust, high-performance self-organizing network. Throughout the course, you'll also find some simple “rules of thumb” and practical pointers to guide you.

Hint

As you go through the topics in this course, watch for answers to these questions:

- How big should your self-organizing network be?
- What effect will plant structures have on where you position wireless devices?
- Where should you put network gateways?
- What best practices can help ensure a successful installation?

*If you haven't already taken the **Self-organizing networks** course, doing so before you begin this course will give you a better understanding of what self-organizing networks are, how they work, and their unique advantages.*

Steps for success

Using a structured approach will help you build a robust self-organizing network and troubleshoot any network issues.

The following steps provide a logical process for easy planning, design, and installation of a self-organizing network that delivers optimal performance:

- Scope the project
- Envision device locations
- Network the devices – on paper
- Integrate the gateway into the system
- Install and commission units
- Fortify the network

We'll look at each step in detail.

Scope the project

The first and most important step in deploying a self-organizing network is to identify what you want to achieve.

For example, is your goal to automate operator rounds by gathering data automatically? Is it to monitor process conditions in areas where installing wired devices would be difficult or otherwise cost-prohibitive? Do you want to gather diagnostic data from existing smart devices?

Having a clear objective will help you focus your efforts – and get the results you want.

It's also best to start with as many wireless devices as practical, in a self-organizing network focused on a single processing unit such as a refinery coker unit or distillation unit. Doing so has three primary benefits:

- It helps ensure that all the wireless devices will be within a reasonable signal range of each other, since they'll be placed in a relatively limited area.
- With several devices in the same area, there are more available communication paths for routing messages around obstructions or other interference.
- It's easier to integrate the data into information systems if all data sources follow the same organizational structure – which in most plants is based on process units.

Depending on how your plant is organized, focusing each self-organizing network on a single unit may also clarify who is responsible for maintaining the devices.

You can add more self-organizing networks as you extend use of the technology to other process units. Large facilities with many units will require multiple networks, while small facilities or a single process unit can probably be managed with a single network.

Envision device locations

Where you will use wireless devices is influenced by their dual role in a self-organizing network: They collect and transmit data, and they serve as routers that pass along communications from other devices.

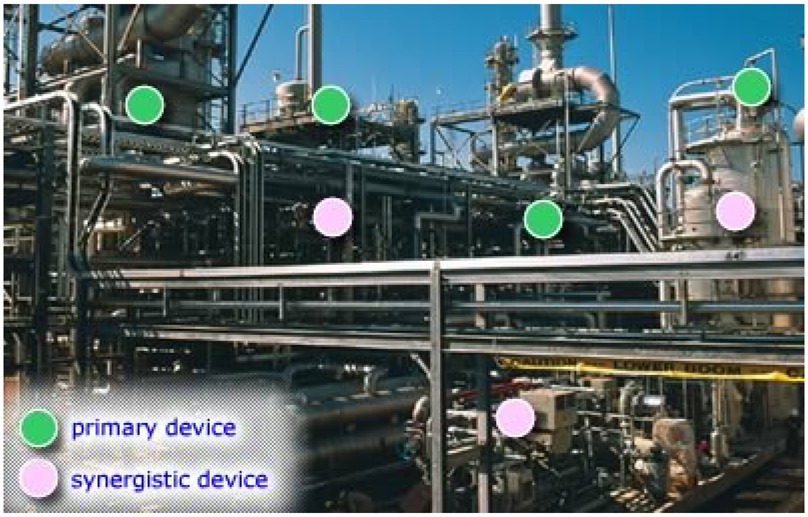
This second role – as routers – requires that the network include enough devices in proximity to each other to support reliable communications when the devices cannot communicate directly with the gateway because of obstructions or distance.

Fortunately, in most applications the natural distribution of measurement points meets this requirement. If not, simply adding a repeater will achieve the same objective.

As you think about potential device placements, consider both your immediate and longer-term goals. Other work groups – such as Operations, Engineering, Maintenance, or Reliability – may also benefit from the information wireless devices can provide.

It's likely that the devices needed to meet your immediate needs will provide enough communication paths for a robust, reliable network. But keeping your long-term goals in mind will enable you to identify opportunities for **synergistic** devices – those that not only provide additional process and equipment data, but also strengthen the network by providing additional communication paths (because they also act as routers for other devices).

Besides helping you brainstorm new ways to optimize process operations, this long-term thinking can also have immediate payoffs.



It's a good idea to identify not only primary device locations to meet your immediate needs, but also where you might put synergistic devices that can strengthen the network while supporting your longer-term goals.

Network the devices – on paper

As explained in the **Self-organizing networks** course, this type of network doesn't require detailed or costly site surveys to identify a line-of-sight path between each device and its assigned gateway. Instead, you can take advantage of the network's ability to automatically route communications around obstacles or other sources of interference.

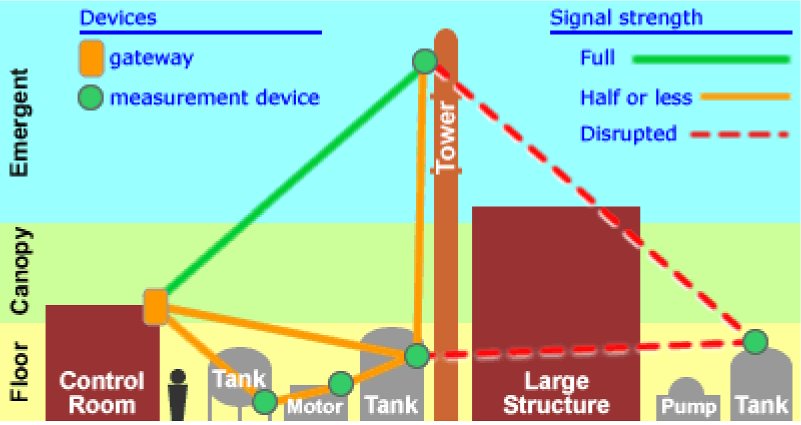
It still makes sense to identify where each device will be located and its available communication paths. That way you can identify likely “impenetrables” – obstructions or areas that a wireless signal can’t get through with adequate signal strength for reliable communications – and plan repeater or synergistic nodes to provide alternate communication paths.

Network the devices – on paper
How impenetrables affect network design

A typical plant includes plenty of potential impenetrables, such as

- Large structures, such as a large building.
- Extremely dense infrastructure, such as piping and girders. If you can’t see through it or walk through it, it's likely a wireless signal won’t get through on its own, either.
- Concrete or metal walls – for example, if one device is inside a building and the others are outside. Concrete will absorb wireless signals, and metal walls will reflect them. Either way, the low-power wireless signals may not get through.
- Transmission distances that exceed the range of the wireless devices.
- Vertical arrangement of devices, since antennas are usually positioned to maximize horizontal signal strength.

Here's an example of how impenetrables affect signal strength.



Impenetrables – such as large buildings or dense infrastructure – can affect wireless transmission range and therefore the design of a self-organizing network.

The diagram shows three vertical layers: floor, canopy, and emergent. Each layer has different potential impenetrables that can affect the network.

In this example plant, the first or **floor** layer – from ground level to about 15-20 feet (5-6 meters) – has very dense infrastructure that reduces signal range by 50% or more. This attenuation depends on the frequency of the radios, as well as the actual density of the environment.

Fortunately, the many potential measurement points in the floor layer mean there are likely to be many wireless devices – providing many alternative communication paths around these impenetrables.

The **canopy** is the layer above motors and pipe racks and below third floor stair decks. It's typically relatively open, but signals may be disrupted by tall structures.

The third layer is occupied by **emergent structures** such as distillation columns or exhaust towers that extend above the canopy. Emergent structures usually have minimal effect on radio signals unless they're part of a larger structure. Extensive testing has also shown that devices mounted in this layer can communicate with devices as far as approximately 160 feet (50 meters) below in the canopy.

At any layer, increasing distance can also weaken signals.

(Keep these potential problems in mind as you continue the course. In a later section we'll show how to solve them.)

Practical pointers

- If impenetrables disrupt direct transmission between wireless devices, simply add synergistic devices to provide alternate communication paths around the disruptions.
- If synergistic devices are not an option, install repeaters in key locations to reinforce the signals and provide alternate paths.

Network the devices – on paper
Using repeaters

You can circumvent obstructions or extend the area where devices can be installed by providing repeater nodes.

Repeaters have the same radio and networking properties as wireless field instruments, but without the measurement capability. Their purpose is to enhance network connectivity.

Practical pointers

- Repeaters perform best in the canopy, where there's easy access to floor-level measurements and relatively open infrastructure allows longer transmission ranges.
- To optimize connectivity, place repeaters about midway between devices that are having trouble communicating with each other.

Well-established networks with many devices should never need repeaters – no matter how dense the infrastructure. But in networks with just a few devices, repeaters can be the key to solving connectivity problems.

Integrate the gateway

Determining how information will get from the gateway to the host system is a critical step in building a self-organizing network.

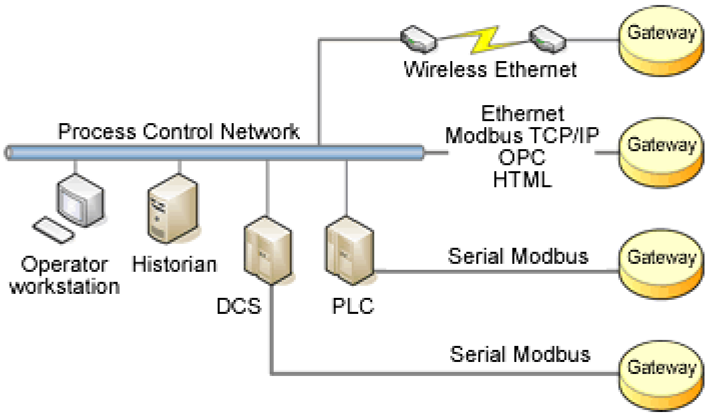
A **gateway** is the interface between a network of wireless devices and a host information system. The connection from the gateway to the host can be either wired or wireless.

Unlike wireless devices that conserve power by spending much of their time in "sleep mode," gateways are always powered to maintain connectivity, manage the self-organizing network, and provide a local user interface.

The **host system** is where most users will access information from the wireless devices. Typical host systems for in-plant applications include distributed control systems (DCSs), programmable logic controllers (PLCs), data historians, and asset management systems.

*For more on gateways, see the course on **Network Components**.*

It's especially important to make sure the gateway can communicate with your host system – or any host system you're likely to have during the life of the network. It's also a good idea to choose gateways that don't require additional proprietary software or modifications to your host system to integrate the data.



Gateways may use different protocols to connect to different host systems.

Practical pointers

If Ethernet is required, a wireless Ethernet connection can be ideal – either through a wireless LAN or a dedicated point-to-point network that spans the distance between the gateway and the host integration point.

Wireless Ethernet provides high bandwidth to handle diagnostic as well as measurement data, and the flexibility of a wireless solution makes optimal placement of the gateway easy. In fact, with a power source as the only requirement, you can place the gateway almost anywhere that's in range of the devices as well as the host connection. For the same reason, it's easy to move the gateway later if needed.

Some applications may require multiple connection types – for example, to support both a DCS and a data historian.

Emerson Advantage

Integration is easy with Emerson's 1420 wireless gateway, which supports a wide variety of standard protocols – including

- **Modbus/RTU** for DCSs and PLCs
- **Modbus/TCP** for DCSs, PLCs, and human-machine interfaces (HMIs)
- **OPC** for data historians and HMIs
- **Ethernet** for asset management systems and other applications on the plant LAN
- **HTTP** for web interfaces used for configuration and simple monitoring
- **XML** and **CSV** (comma-separated values) for bulk data transfer

Install the network

There are two key points to keep in mind when you build your first self-organizing network:

- Install the gateway first.
- Install wireless devices nearest the gateway first, then expand outward.

Installing the gateway

The gateway is the backbone of the network. Installing it first enables you to check for proper operation of each device as it's added to the network and begins communicating with the gateway.

The gateway should be placed in a central location to maximize the number of devices it can communicate with directly. If that's not an option, place it near the closest wired integration point.

Practical pointers

- For the highest signal quality, install the gateway outdoors. (In this case, a minimum rating of Class I Div II or Zone 2 is required).
- Install the gateway at least 3 ft (1 m) above other structures in the canopy (for example, above the roof of a control room).
- If outdoor mounting is not an option, connect the gateway to a remote omni-directional antenna using a cable no longer than 20 ft (6 m).

Installing wireless devices

Install devices starting with those closest to the gateway, then work outward from that point. Once you verify that the first devices are working, you'll be confident of a reliable communication path for those you add next – and a solid foundation for expanding the network. You can use repeaters to temporarily strengthen the network until all the devices are installed or until the network completely surrounds an entire process unit.

To avoid a single point of failure, it's good practice for even the smallest networks to have at least two devices that can communicate directly with the gateway without intermediate "hops." For large networks, the rule of thumb is one additional directly connected device for every eight devices in the network. You may also choose to install redundant gateways.

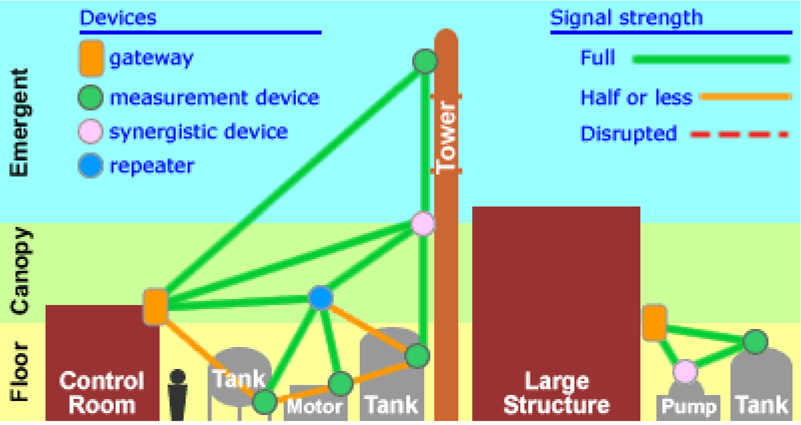
The wireless devices have the same process connections, instrument mounting, and instrument locations as traditional wired HART devices, so you can use existing instrument-commissioning practices. You can also calibrate the sensors using the same configuration tools as for traditional HART devices.

Once the devices are installed, they will automatically join the network, self organize – to find the best route for transmission – and deliver messages to the gateway.

Practical pointers

- Orient all antennas vertically.
- To maximize sensitivity of a wireless device's antenna, make sure the antenna is not directly adjacent or parallel to a conductive surface. A good rule of thumb is to keep device antennas at least a forearm's-length away from infrastructure like boiler walls or fan shrouds.
- After installation, you should never have to "tweak" the device or antenna position to improve the connection. The presence of other nearby devices in the network will provide adequate connectivity.

You'll remember than in an earlier section of this course we showed how impenetrable structures could block or reduce the reliability of wireless signals. Here's how that same plant could avoid those problems with repeaters and proper placement of gateways.



The gateway on the left is installed outside and above a control room to maximize connectivity with the network. A repeater in a potentially “weak signal” area improves connectivity to devices in the dense infrastructure of the plant floor and provides additional connectivity to the gateway. The gateway on the right serves devices that can't communicate wirelessly with those on the left because the large structure blocks the signals.

Fortify the network

Once the network is up and running, two simple steps will help ensure that you have a robust and reliable solution – not just today, but for the long term.

First, verify that each device has joined the network and is communicating properly. If a communication link can’t be made, you can add synergistic devices or repeaters to bridge the connection to the network.

Next, identify any “pinch points.” If messages from several wireless devices must all pass through a single device or repeater at any point on their way to the gateway, the network becomes “pinched” – creating a single point of failure that can compromise the network's long-term reliability.

This doesn't happen often because of all the redundant communication paths in most self-organizing networks. But if it does, some networks can generate an alert to inform you, and you can then simply add additional devices or repeaters near the pinch point to provide additional communication paths.

Practical pointers

The wireless devices in your self-organizing network have good connections if…

- At least 99% of messages sent by each device reach the assigned gateway.
- At least 70% of transmissions between two nodes (one "hop") are successful.
- Data latency (time from when a message leaves a device until it reaches the gateway) is less than 1/3 the update rate. For an update rate of 60 seconds, for example, that means each message takes no more than 20 seconds to reach the gateway.
- Device batteries last as long as expected. (But note that battery life can be also be affected by other factors. See the course on Power Management for details.)
- Radio Signal Strength Indication in the gateway diagnostics is good. This check is listed last because it can be misleading on its own (weak signals can still get through if the path is stable), but it can help identify a problem when it arises.

Expanding the network

When it comes to self-organizing networks, bigger is better. In fact, the more wireless nodes in the network, the easier it is to expand. That's because there are so many available paths for the additional communications to follow. The network simply senses that a device has joined the network, and routing algorithms in the devices and gateways automatically find the best route to a destination.

Think of the existing network as providing a giant antenna for any new device you add to the periphery of the network, and a myriad of connections available for one you add to the interior. The only limitation is the amount of traffic that can be handled by each gateway and by the devices that provide the last "hop" to it.

This capability makes not only large-scale additions easy, but also the addition of single points to meet short-term needs. You can even install a temporary device to test whether a permanent installation would add value, or to do short-term monitoring for diagnostic purposes.

Troubleshooting

Self-organizing networks are highly dependable, but – as with any system – individual components can be affected by equipment failures, installation and commissioning errors, or changing conditions.

Fortunately, good wireless devices have built-in diagnostics to automatically identify (or even predict) potential problems. These include diagnostics not only for the device's sensor, but also its battery and wireless communications.

Let’s say a device you've just installed fails to join the network. Its diagnostics enable you to first determine whether the radio is working. If it is, then either ...

- the network ID in the device doesn't match the ID of the network it's trying to join (a security safeguard), in which case, you can reconfigure the device's network ID, or
- the device is out of range – a problem you can solve by adding another device or a repeater to establish connectivity.

A high-quality gateway can also provide diagnostic information for troubleshooting connectivity problems. Together with a layout of existing devices and impenetrables, this information can help you determine where to put additional devices or repeaters – or in the worst case, where to reposition the gateway and use wireless Ethernet to link it back to the rack room or other connection point.

When very small networks are first being deployed in a plant, it's not unusual to have some connectivity problems if the devices are sparsely distributed. Fortunately, this is an easy problem to resolve. You can minimize these connectivity issues by

- installing repeaters or synergistic wireless devices.
- ensuring there are multiple wireless devices that connect directly to each gateway.

The best way to avoid networking and connectivity problems is to confine each self-organizing network to a specific area – such as a single process unit – and install as many devices as possible. It’s that simple.

Emerson Advantage

Emerson has been a leader in providing useful diagnostics in field instruments. Our wireless devices have many of the same capabilities – and more.

Our 1420 gateway also provides a wide range of diagnostics to help with network installation, troubleshooting, and maintenance. Examples include

- Path statistics (per channel)
- End-to-end message reliability
- Radio Signal Strength Indication
- Link Quality Index
- Live List (which devices are "alive")

It also provides access to field-device diagnostic data, such as battery voltage, alarm indications, and loss of connection, as well as traditional HART sensor diagnostics.

Summary

This course has covered a lot of ground, but the multi-step process it outlines makes planning and installing a self-organizing network a logical, easy-to-manage task.

One thing is clear: the best way to achieve a successful installation is to take advantage of a self-organizing network's built-in capabilities. Other key points include:

Scope the project	Define your goals. Focus on one process unit.
Envision device locations	Besides devices needed to meet your immediate objectives, plan for future synergistic devices that can add more measurement points while also strengthening the network.
Network the devices – on paper	Identify impenetrables and how the network will deal with them. If necessary, add more devices or repeaters to your plan.
Integrate the gateway	Select a gateway that can integrate seamlessly with your host systems.
Install the network	Follow guidelines for installing gateways and devices to maximize network reliability.
Fortify the network	Verify that all devices are communicating. Add devices or repeaters to bridge weak connections and eliminate pinch points.
Expand the network	The bigger the network, the easier it is to expand.
Troubleshooting	Use built-in diagnostics to identify problems.

Your wireless-network supplier can also provide additional tips based on experience with similar installations.

Emerson Advantage

As a leader in wireless solutions for process automation, Emerson has extensive experience planning and installing self-organizing networks. You can use our services to supplement your own engineering and installation teams, or to provide a completely installed network tailored to your needs.

Emerson also offers a Wireless SmartPack™ Starter Kit that includes your choice of 5-100 Rosemount wireless measurement devices; a 1420 gateway; AMS Device Manager software, and our SmartStart™ wireless installation services. Pre-configured to form a self-organizing network right out of the box, the SmartPack provides an easy, low-cost way to gain practical experience with wireless technology in your own facility.