Wireless Ethernet Solution in an Industrial Automation I/O Network

Erik Westberg
Pfizer
Senior Automation Engineer
10 December 2015

Connecting a World of Pharmaceutical Knowledge

Pfizer Biotech

Overview

Where do we use wireless Ethernet for automation purposes?

- To connect workstations to our control system.
  - Mobile workstations provide users with greater access to the Manufacturing Control System (MCS) than fixed locations.
  - This portable access allows for remote monitoring and response to critical alarms during off shift hours.
  - These connections leverage corporate infrastructure including the wireless network and allow for use of VPN access.
- To connect skids to our control system
  - Portable skids help create a flexible dynamic processing area capable of being reconfigured as required.
- To connect distributed I/O to our control system
  - Replacement of standard wired Ethernet I/O networks to improve flexibility and mobility.

Overview continued

This presentation will focus on the use of wireless Ethernet for connection of distributed I/O and Skids to the MCS.

- Why did we choose to go wireless
  - Cost vs. Flexibility
- Physical Control System overview
  - Hardware overview
  - Network connection
- Risk assessment
  - Security
  - Capabilities
    - Data collection
    - Control
    - Robustness
- Lessons learned

Why do We Use Wireless

Why and how do we use wireless Ethernet

- In order to meet plan of record we needed to provide a solution for connecting portable equipment to our MCS.
  - The portable equipment could be placed anywhere in the given suite.
  - Several skids may be in the same room at a given time.
  - The equipment may also need to be reconfigured quickly to allow for changes to process as required by different products.
- The nature of the skids requires operators to move around them regularly making any cabling additional trip hazards.
  - Tripping on these cables can cause damage to cables and connectors, loss of product, or worse personnel injury.

Why do We Use Wireless cont.

- By removing the requirement for Ethernet cables we accomplish the following.
  - Trip hazards are reduced.
  - Equipment becomes more mobile and flexible allowing for improved process changes.
  - Reduced suite down time related to moving skids.
  - Reduced suite down time related to dirty work of cabling installation and repair.
  - Reduction in data loss caused by damaged cables and connectors

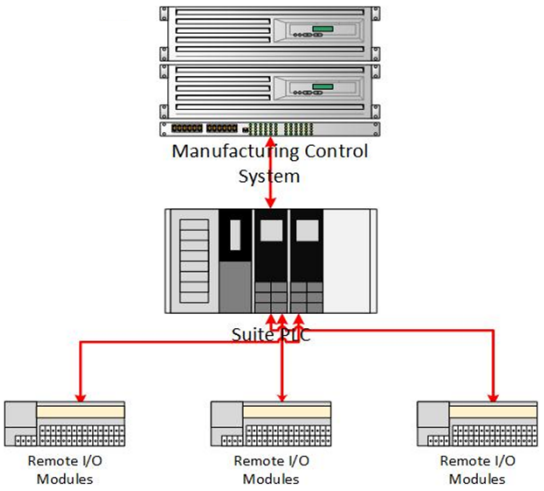
Why do We Use Wireless cont.

Installation cost was not a significant deciding factor in this installation

- The one time installation cost of installing as many access points as were installed as part of this project was significantly more than installing 3 Ethernet cables to each room in the suite.
  - This installation cost may be different if fewer access points are needed.
- The biggest benefit of this system is allowing the mobility of the portable equipment while minimizing repair costs and down time.
  - There is a significant cost to installation, repair and replacement of traditional wired Ethernet networks.
  - There is significant cost associated with down time and dirty work inside of a manufacturing suite.

Physical Control System Overview

Our example network consists of an MCS layer, a PLC, and distributed remote I/O modules.



Physical Control System Overview cont.
The PLC

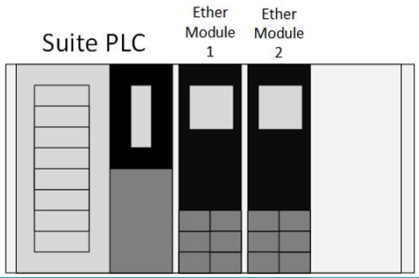
The PLC is configured with 2 separate Ethernet modules.

The PLC communicates to both Ethernet modules via the backplane.

- The first module is used to allow the MCS to connect to the PLC.
- The second is used to allow the PLC to communicate with the distributed I/O.

Additionally the MCS can communicate through E-net 1 to E-net 2 using the PLC backplane as a gateway.

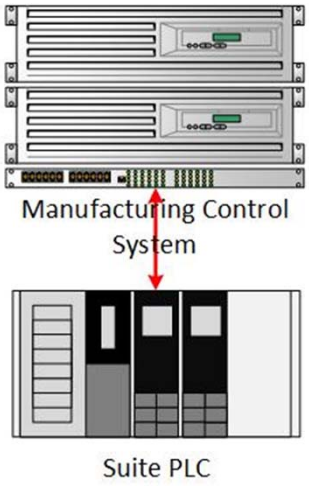
- This allows MCS to connect to anything that can be added to the I/O network including fully automated skids.



Physical Control System Overview cont.
The MCS to PLC Connection

The MCS communicates to the PLC via wired Ethernet through E-net 1.

This allows data that is polled by the PLC to be transmitted to the SCADA system to be viewed real time and stored for historical review.

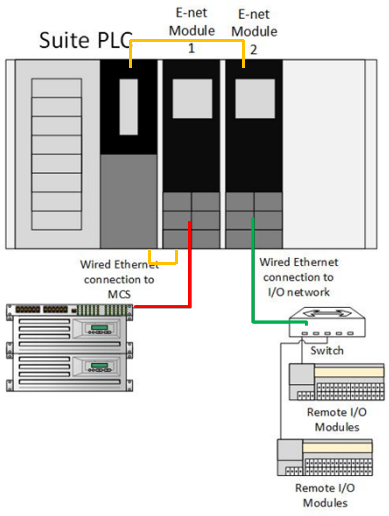


Physical Control System Overview cont.
The Industrial I/O Network

The second Ethernet module, E-net 2 is used for the Suite PLC to communicate with remote I/O modules configured in the PLC.

The I/O values then are read by the PLC.

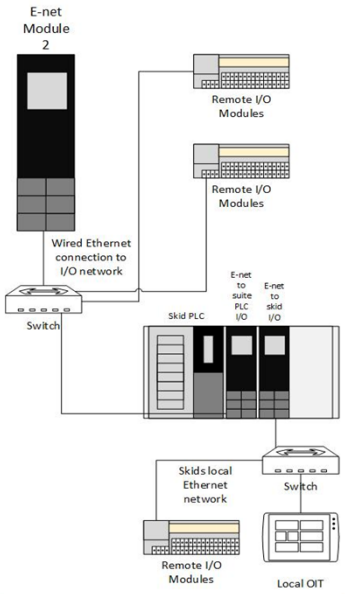
The MCS then polls the data via the primary Ethernet module.



Physical Control System Overview cont.
The Industrial I/O Network

Additionally we can connect fully self contained skids to the I/O network.

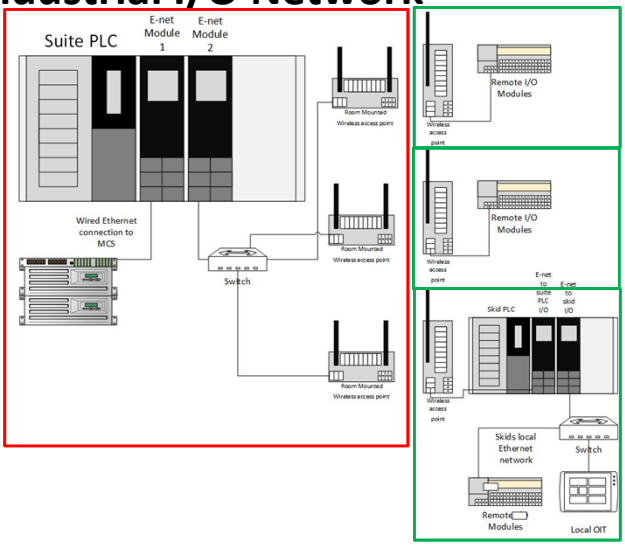
- Using the correct I/O drivers installed on the MCS we can tunnel from E-net 1 to E-net 2 through the PLC's backplane without involving the Suite PLC.
- Thus using the PLC backplane as a gateway creating a segregated Ethernet network.
- The skid needs to be configured similar to the Suite PLC with 2 Ethernet modules, one for the skids local Ethernet network and one for the Suite PLC I/O network.



Physical Control System Overview cont.
The Industrial I/O Network

By replacing the traditionally wired connections between the I/O network and the portable skids with wireless access points we remove trip hazards, prevent cable and jack breakage, allow for more portability, and prevent the need to run multiple cables to each room.

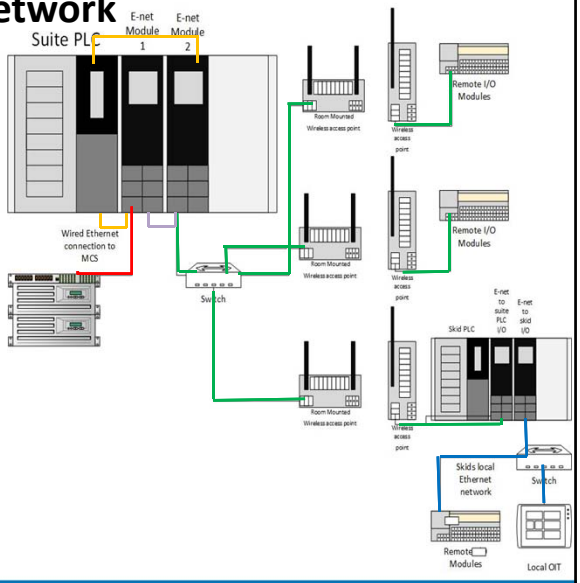
The red box indicates fixed components and the green box indicates portable equipment.



Physical Control System Overview cont.
The Industrial I/O Network

Communication

- The MCS to PLC coms is hardwired and shown in red.
- The backplane coms between the PLC and Ethernet modules is indicated in Orange.
- The "Gateway" backplane coms from E-net 1 to E-net 2 is indicated in purple.
- The portable skid network is hardwired wired and shown in blue.
- The Suite PLC I/O network is a mix of hardwired and wireless is indicated in green.



Risk Assessments: Security

Several different approaches were used to address security concerns on the wireless network.

- The access points used had a variety of security configurations that can be enabled.
  - Enable network password protection.
  - Disable SSID Broadcasting
  - Signal broadcast strength
    - By setting the broadcast strength low the signal could not be picked up in adjoining rooms let alone non-secured portions of the site.

Risk Assessments: Data Collection Capabilities

Would the wireless network have the bandwidth and communications rate capable of collecting the required data?
Traditional RF serial coms had been tested and did not meet needs.

- The wireless network showed the ability to collect data at 1 second intervals from as many as 9 separate skids at the same time.
  - The initial skids installed were strictly data collection from remote I/O modules.
- As we became more comfortable we added the ability to collect data from the self contained skids using the Ethernet to Ethernet gateway.
  - The addition of more skids showed no signs of impacting data collection.

Risk Assessments: Control Capabilities

Would the wireless network be capable of control?

- As the use of the network expanded the idea of control over the network was explored.
- The network was evaluated against existing hardwired networks for communication rates and number of failed or errored transactions.
  - There was no significant difference between existing wired Ethernet control networks and the wireless Ethernet network.
- Some minor control over the wireless Ethernet was enabled.
  - Care was taken to ensure communications loss would not result in any safety incidents.

Risk Assessments: Robustness Capabilities

Would the wireless network be robust enough to support ongoing operations?

- Commissioning showed that in the event that an access point went down that the remaining access points did over lap enough to allow communications to continue.
- Remote I/O skids were configured with local alarm to notify an operator if the connection was lost.
  - This alarm originally would also enable a local chart recorder to capture data. The chart recorders were removed once the network showed to be effective.
- Heartbeat signals were added to self-contained skids to alarm like the remote I/O skids. At this point there was no need for local collection.

Lessons Learned

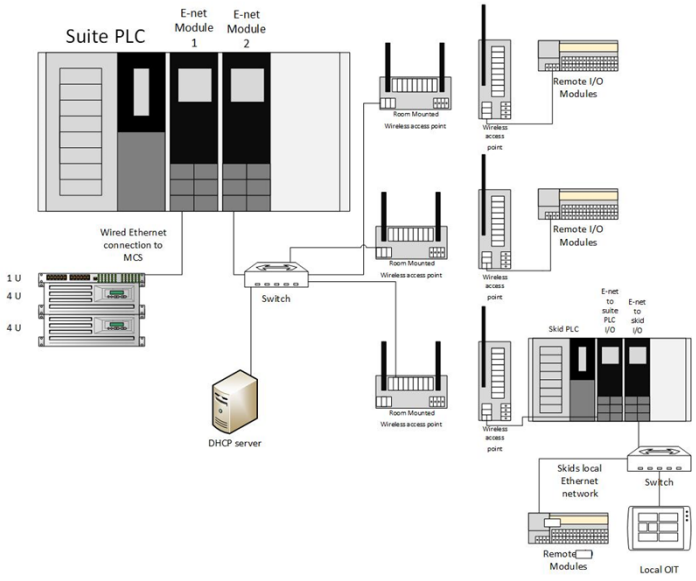
From conception through the first few years of operation we ran into several issues.

- Wireless signal overlap causing data drops.
  - By reducing the broadcast power further the signal did not overlap as much preventing the hopping from access point to access point.
  - Initial commissioning runs had the broadcast power set slightly higher than final installation.
  - When skids were between access points the signal would jump back and forth causing momentary losses in data.
- BT wireless network causing interruptions
  - After our initial installation our BT department changed the wireless network protocol they were using.
  - This change was to the same protocol that our wireless network used.
  - The addition of the new network caused disruptions to our control network.
  - As a result we needed to change out all of our hardware to access points that could be configured to multiple protocols.

Lessons Learned cont.

- As with any Ethernet networks duplicate IP addresses can cause problems.
- For the PLC Ethernet module it is a bigger problem as the modules fault and can not recover, they need to be rebooted.
  - As more equipment was added to the network we started to see occasional network failures from duplicate IP addresses on the network.
  - Unlike many computers the Ethernet module could not recover from the error without being rebooted.
  - As a result an imbedded computer was added to the network and set up to be a DHCP server. All equipment on the network now get their IP from the DHCP server, limiting the change of duplicates.

Lessons Learned cont.



Lessons Learned cont.

- Operations personnel might not be aware of signal loss
  - On the skids that are remote I/O connected to the suite PLC we had a very simple solution.
    - We used a discrete output configured to fail low connected to a relay that was used to enable a buzzer located on the skid.
    - The discrete output was set high by the PLC. In the event that connection to the skid was lost the output would fail low enabling the buzzer.
  - On the self contained skids that are capable of running without connection to the PLC a different approach needs to be used.
    - In this case a heartbeat tag was added between the skids local PLC and the MCS. This heartbeat would be used to enable a local buzzer.

Commissioning and Validation

- Once all of the access points were installed we did a survey to determine the broadcast power and adjust where the signal could be picked up.
  - This was used as part of our security assessment
  - Limiting detection of the wireless signal to inside the desired suite was the goal.
- One significant benefit of this design was the use of Ethernet I/O modules which had already been used here on site.
  - As a result no additional testing was required as the modules had already been approved.
  - Our standard I/O to SCADA display test was able to verify the data connection.
  - A verification of trending was used to verify consistency of connection.
- All data collection from these devices has been qualified for GMP uses.

Summary

- Operations group raised a requirement for portable equipment.
- Requirement led to modifying a tried Ethernet I/O network by leveraging wireless access points to replace traditional hardwired connections.
- Testing and use led to modification in broadcast power, changes to broadcast protocol, and addition of DHCP server.
- Skids are now extremely flexible in terms of mobility and have very consistent connection to data collection.