White Paper - Secure Wireless Ethernet for Fuel Dispenser EMV

Version:	2
Created:	March 29, 2018
Modified:	March 29, 2018
Author:	Bob Danford

ALLIED
WIRELESS

Allied Electronics, Inc.
1414 Radcliffe Street Suite 120
Bristol, PA

voice: 215-785-6200
e-mail: BobD@AlliedElectronics.com

Revision History

Version 2	*29 March 2018* *BD*

Table of Contents

1 Introduction

In retail fueling centers, there is a component that is often referred to as the forecourt. For the purposes of this paper, the forecourt is defined to include the following items:

- Fueling dispensers and in-dispenser payment terminals (DPTs)
- All devices contained within the fueling dispensers (displays, printers, cash acceptors, barcode readers, etc.)
- Island Payment Terminals (IPT)
- Change Back Machines (CBM)
- Leak detection systems
- Car wash controller systems
- Electronic price signs
- Debit processing systems for pay at the pump (PAP)
- Card processing networks (optional)

Within this environment, one of two paths is taken for connectivity when migrating to EMV:

1. Media conversion over legacy existing wires.
   a TCP/IP over RS485
   b Homeport (Data over power line).

2. Secure Wireless Ethernet

This white paper illustrates the benefits of utilizing Secure Wireless Ethernet when interfacing with next generation EMV payment in the forecourt. The Allied Wireless line of Secure Wireless Ethernet products will be used as the basis for details. The benefits will be broken down into the following subject areas:

- Forecourt data and networking challenges
- Encryption and Security
- Bandwidth and Reliability

2 Forecourt Data and Networking Challenges

Why is forecourt network connectivity so burdensome?

- Existing wiring in most forecourts is comprised of aging and buried 2 or 4 wires which are capable of only current loop or serial data transmission.

- Dispensers, DPTs and Island Payment Terminals (IPTs) require constant polling. This places excessive bandwidth requirements on the low bandwidth existing wires.

- Forecourt devices present proprietary software and electrical interfaces such as current loop. Current loop, for example, was never designed to be transferred over TCP/IP and is often a significant bottleneck when considering a move to networked forecourt devices, such as EMV payment systems.

- As the number of forecourt devices (e.g. dispensers, digital media and EMV card readers) increases, the burden on the aging 2 or 4 wires increases significantly.

- The ability to network all forecourt devices such as DPTs, displays, printers, cash acceptors, barcode readers, IPT's, CBM's, leak detection systems, car wash controller systems, electronic price signs, and EMV PAP systems is severely limited by the wide variety of unique data types along with the bandwidth restrictions of the aging 2 or 4 buried wires.

- Security requirements for each device in the forecourt varies. For example, PCI rules for network credit card payments require much more stringent security standards than those of an electronic price sign or leak detection system.

How does Secure Wireless Ethernet for fuel dispenser EMV help?

- By installing a UL 1238 certified secure wireless device inside the fuel dispenser, the need to transmit over the aging 2 or 4 wires is eliminated completely.

- Installation of insecure wireless devices inside the dispenser requires a fraction of the time vs. IP over RS485 or Home Port technology. The secure wireless "plug and play" technology requires no previous networking or wireless set up experience, making it simple for Authorized Service Technicians to install in a matter of minutes vs. hours, which reduces costs and downtime.

- Since the wireless is digital TCP/IP and highly encrypted, issues such as noise, loop back failures, and security issues are virtually eliminated.

- When combined with the Allied Current Loop & Serial to Ethernet adapter, an installer is able to quickly and easily connect other non-TCP/IP devices in the dispenser to one of 4 ports of the integrated managed Ethernet switch inside the secure wireless system. This offers WAN/Cloud management for virtually any aspect of the fuel dispenser or forecourt devices.

- Secure Wireless Ethernet devices are designed to be highly scalable. Increasing the number of fueling points or card reader devices does not slow down the system.

3 Encryption and Security

In today's world, credit cards and personal information are routinely sent through "exposed connections" such as the Internet, WLANs and Cellular phones when using EMV credit cards, or online through secure websites. These credit transactions and a user's personal information are safe because the data transferred is highly encrypted between the client device and the bank or website via technologies called Transport Layer Security (TLS) and Secure Sockets Layer (SSL) over HTTPS.

In addition however, Allied's Secure Wireless Ethernet encrypts all data with the US government's FIPS 197 - AES encryption cyphers. These cyphers have been the standard for US Military's Secret Level communications since approval in 2002.

- This encryption provides extra secure confidentiality of all data transferred across the wireless connection. This is critically important for "insecure" swiped credit cards, personal sessions and other network data that are not using the aforementioned EMV, TLS, SSL and HTTPS technologies.

- Whenever Allied Wireless transmits any data; EMV, TLS, SSL or raw, it gets encrypted. Thus, transmissions of EMV, TLS, SSL and HTTPS are considered "double encrypted" which is highly more secure against hacking attempts.

A Secure Wireless Ethernet solution is capable of delivering the high speeds necessary to accommodate next generation fuel dispensers – along with fully certified data encryption technology and VLAN (virtual local area networks) segmented switching. It is this segmentation that is also critical to establishing a secure wireless payment infrastructure.

- VLAN segmentation works by creating a collection of isolated networks, each with a separate broadcast domain, within a data network. This segmentation within a VLAN network adds yet another level of security by blocking access from malicious attackers against the system. In addition, it eliminates packet-sniffing attempts, which are sometimes used by outside agitators to capture network traffic at the Ethernet frame level in order to retrieve sensitive information such as financial data. With VLAN segmentation, only authorized personnel can access the servers and various digital devices necessary to execute payment transactions.

4 Bandwidth and Reliability

Bandwidth and throughput are common determinations for how fast and how much data can travel across any medium (wired or wireless). It is not uncommon to see specifications of "20 or 40 Mbps" bandwidth claims for technologies such as IP over RS485 or Homeport (Data over power line). While theoretically these bandwidths are true, the actual throughput is significantly less due to "real world" conditions such as noise, the condition of the aging wiring, conversion inefficiencies, etc., etc. It is not uncommon to see little more than 1 Mbps of actual throughput on systems such as these.

- With Secure Wireless Ethernet, real usable throughput is much higher than either of these two methods. While over air bandwidth is typically calculated at 300 Mbps for Secure Wireless Ethernet systems, the user can expect no less than 150 Mbps of actual usable throughput. For the forecourt this is more than enough throughput and speed for today's demands as well as the fuel dispenser and forecourt of the future, which will include features such as digital media, IP cameras, and EMV payment requirements.

Reliability of any wireless system is based on how much power is transmitted. The Allied Secure Wireless Ethernet solution utilizes the latest most powerful technology from Qualcomm along with the maximum legal transmit power allowed by the FCC (1W).

- What this means in a real world implementation is that the Allied Secure Wireless Ethernet system is capable of over a mile of reliable range. Since most forecourts are measured in hundreds of feet, the system has more than enough power to insure 24/7/365 connection without issue. This means tankers and any other vehicles or obstructions in the path of the radio transmission WILL NOT degrade the connection. The 1W power and multipath technology combine to make the connection as reliable as a buried Ethernet cable.

5 Conclusions

To achieve Payment Card Industry (PCI) compliance, American fuel centers are making the switch to EMV pump payment systems. In the process, many are discovering that installing a Secure Wireless Ethernet network for their complex needs allows them to avoid the costly expense and downtime associated with a wired system. A Secure Wireless Ethernet solution is capable of delivering the high speeds necessary to accommodate next generation fuel dispensers – along with fully certified data encryption technology and VLAN (virtual local area networks) segmented switching. It is this combination of speed, encryption, and integrated managed switch with VLAN segmentation that is critical to establishing a robust and secure wireless payment infrastructure and why some of the largest US retailers have deployed the Allied Electronics Secure Wireless Ethernet system for Fuel Dispenser EMV upgrades.