PoE Microgrid for Commercial Buildings Lab Evaluation

Final Report

ET23SWE0053

Prepared by:

Keith Graeber CLTC

Andrew Harper CLTC

December 20, 2024

Acknowledgements

Disclaimer

The CalNEXT program is designed and implemented by Cohen Ventures, Inc., DBA Energy Solutions (“Energy Solutions”). Southern California Edison Company, on behalf of itself, Pacific Gas and Electric Company, and San Diego Gas & Electric® Company (collectively, the “CA Electric IOUs”), has contracted with Energy Solutions for CalNEXT. CalNEXT is available in each of the CA Electric IOU’s service territories. Customers who participate in CalNEXT are under individual agreements between the customer and Energy Solutions or Energy Solutions’ subcontractors (Terms of Use). The CA Electric IOUs are not parties to, nor guarantors of, any Terms of Use with Energy Solutions. The CA Electric IOUs have no contractual obligation, directly or indirectly, to the customer. The CA Electric IOUs are not liable for any actions or inactions of Energy Solutions, or any distributor, vendor, installer, or manufacturer of product(s) offered through CalNEXT. The CA Electric IOUs do not recommend, endorse, qualify, guarantee, or make any representations or warranties (express or implied) regarding the findings, services, work, quality, financial stability, or performance of Energy Solutions or any of Energy Solutions’ distributors, contractors, subcontractors, installers of products, or any product brand listed on Energy Solutions’ website or provided, directly or indirectly, by Energy Solutions. If applicable, prior to entering into any Terms of Use, customers should thoroughly review the terms and conditions of such Terms of Use so they are fully informed of their rights and obligations under the Terms of Use, and should perform their own research and due diligence, and obtain multiple bids or quotes when seeking a contractor to perform work of any type.

Abbreviations and Acronyms

Acronym	Meaning
AP	Access Point
CT	Current Transformer
DAC	Disadvantaged Communities
EE	Energy Efficiency
ET	Emerging Technology
GHG	Greenhouse Gas
HP	Heat Pump
HTR	Hard-to-Reach
HVAC	Heating, Ventilation, and Air Conditioning
IEEE 802.3af/at/bt	Power over Ethernet Standards
IOU	Investor-Owned Utility
IT	Information Technology
kWh	Kilowatt-hour
PA	Program Administrator
PAC	Physical Access Control System
PD	Powered Device
PG&E	Pacific Gas & Electric
PoE	Power Over Ethernet
PSE	Power Sourcing Equipment
SCE	Southern California Edison
SDG&E	San Diego Gas & Electric

Acronym	Meaning
TPM	Technology Priority Map
WH	Water Heating

Table of Contents

List of Tables

List of Figures

Executive Summary

The purpose of this study is to evaluate the efficiency and cybersecurity of Power over Ethernet (PoE) building control systems compared with traditional AC-powered systems. As the adoption rates of PoE technology continues to grow across building automation systems, the study sought to assess the technical and operational performance of various PoE-enabled devices, providing insights into both their electrical efficiency and cybersecurity posture. The study's goals include identifying how PoE systems can streamline power and communication infrastructure in commercial buildings, while addressing any associated cybersecurity risks.

The research team began the study with a market assessment that aimed to identify a diverse set of PoE-enabled devices to evaluate both their efficiency and security characteristics. The primary goals of the market study were to examine the availability of PoE enabled building system components, to determine the range of power requirements across different PoE building systems, and to evaluate the market trends towards PoE adoption in critical systems like lighting, HVAC, and IT infrastructure. This evaluation revealed an increased presence of higher-power Power Sourcing Equipment (PSE), supporting the advanced power needs of modern PoE devices. The assessment pinpointed a significant shift towards PoE integration among large lighting manufacturers and highlighted the availability of PoE solutions designed to retrofit existing systems. Notably, advancements in PoE specifications, such as IEEE 802.3bt Type 4, enabling up to 90 watts per port, have facilitated this broad adoption. The study also highlighted the availability of PoE switches with varied capacities, underscoring the efficiency benefits of aligning switch output with anticipated device loads. This market assessment underscored PoE technology's growing market share in building controls technologies.

After the PoE devices were selected and procured per the market assessment, the team initiated a comprehensive electrical analysis to evaluate the power consumption, system efficiencies, and performance characteristics of various PoE devices, including PoE cameras, PoE physical access controllers (PAC), PoE Mini PCs, and PoE LED luminaire drivers. This analysis involved multiple test phases: comparing PoE versus AC system efficiencies, assessing switch efficiencies under various load conditions, and evaluating the efficiency of centralized versus decentralized architectures.

When comparing PoE systems powered by PSE 5 and PSE 2 switches to traditional AC power systems, PoE systems exhibited lower total system efficiency due to the significant power consumption of the switches and the inherent power loss in PoE nodes. For example, the PoE Camera powered by the PSE 5 switch showed a system efficiency of 41 percent, whereas the AC-powered version achieved an efficiency of 84 percent (Table 1). Similarly, Mini PCs powered by PoE exhibited lower efficiencies compared to their AC counterparts (65 percent vs. 89 percent).

PSE	PD Type	Quantity Tested	Switch Load Percentage (%)	Switch Efficiency (%)	Total System Efficiency (%)
PSE 5	PoE Camera	4	2%	N/A	41%
	PoE PAC	4	6%	N/A	61%
	PoE Mini PC	8	20%	79%	65%
	PoE USBC Charging[1]	4	91%	N/A	95%
	PoE LED Troffer	8	88%	87%	80%
	PoE Shade	1	0.7%	N/A	61%[2]
PSE 2	PoE Camera	4	6%	N/A	37%
	PoE PA	4	20%	N/A	62%
	PoE Mini PC	4	33%	74%	59%
	PoE VAV Controller	2	13%	N/A	65%

PSE	PD Type	Quantity Tested	Total System Efficiency (%)
AC Wall Adapter	AC Camera	1	84%
	AC PAC	1	92%
	AC Mini PC	1	89%
	AC USBC Charging	1	87%
	AC LED Troffer	1	91%
	AC Shade	1	67%
	AC VAV Controller	1	87%

Table 1. Summary of PoE and AC System Electrical Efficiencies

The team analyzed switch efficiencies across various load profiles, finding that efficiency generally increased as load on the switch increased, even though these efficiencies include some fluctuations at higher loads. For example, the PSE 2 achieved 49 percent efficiency at an 11 percent load, which improved to 83 percent at 91 percent load (Figure 1). However, certain switches, like the PSE 1, exhibited optimal efficiency within a mid-load range, with efficiency peaking at 79 percent at a 67 percent load before dropping to 69 percent at an 84 percent load. This suggests that while switch efficiency improves with increased load, it may plateau or decline as the switch approaches full capacity. These findings highlight the importance of managing switch loads to optimize system efficiency, particularly in PoE applications where power distribution can vary significantly based on the specific devices connected.

---

[1] USBC Charging devices were tested on the PSE 4 switch

[2] The efficiency value of 61% was calculated based on results from lab testing where only 1 shade device was powered and metered.

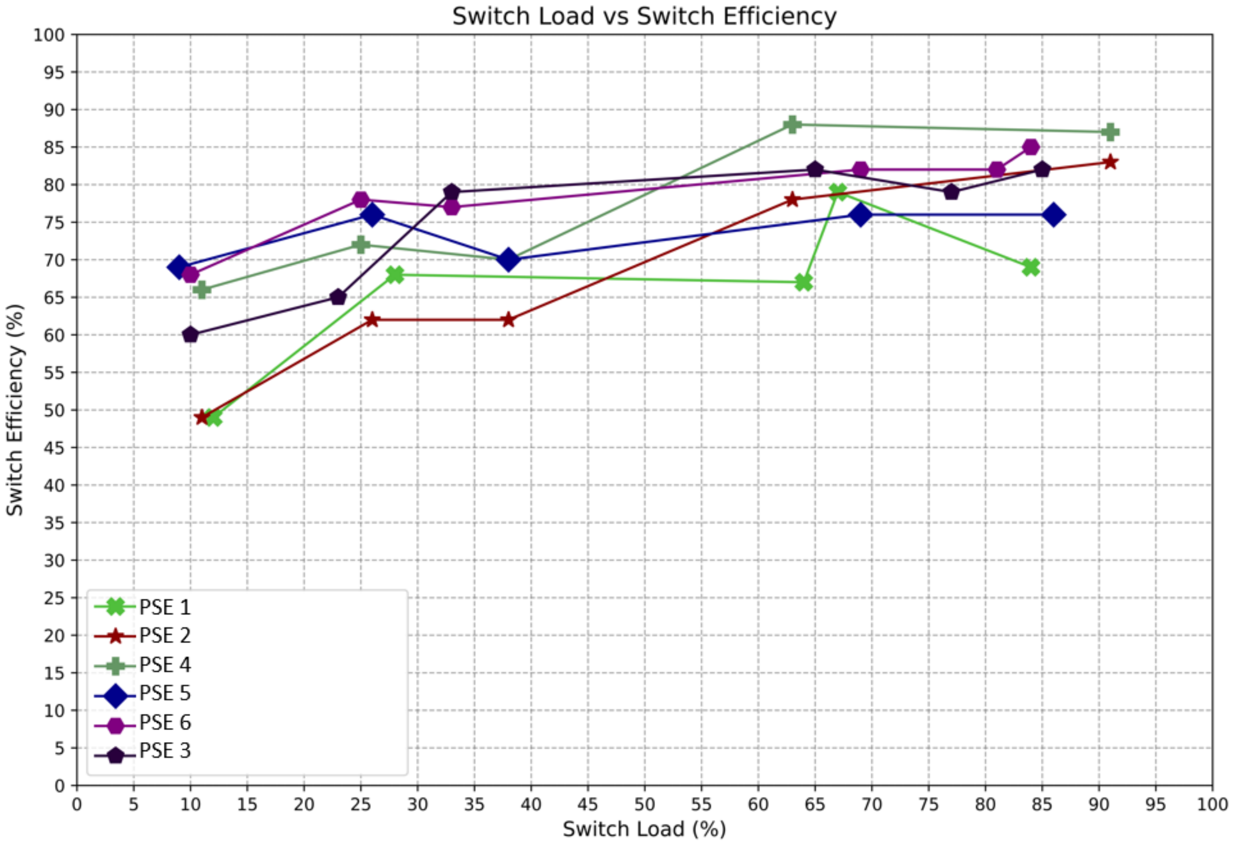

Figure 1. Switch Efficiency with Increasing Load

Finally, the study compared the efficiencies of centralized and decentralized PoE architectures, both of which utilized the same types and quantities of PoE devices (Table 3). The results indicated that centralized systems, such as those using large switches like the PSE 3 and PSE 6, demonstrated significantly better efficiency, achieving 77-80 percent efficiency compared to 74 percent in decentralized systems. This performance advantage is largely attributed to the reduced overhead in centralized configurations, where a single large switch manages multiple loads more effectively. In centralized systems, the computational overhead required to manage PoE functionality is distributed across the entire load, minimizing its impact on overall efficiency.

Table 2. Summary of Centralized vs. Decentralized Architecture Efficiencies

PSE Type	PD Type	Quantity Tested	Total End Point Load (W)	Total System Load (W)	System Efficiency
PSE 6	PoE Camera	4	846	1062	80%
	PoE PAC	4			
	PoE Mini PC	8			
	PoE LED Troffer	8			
PSE 3	PoE Camera	4	837	1061	77%

	PoE PAC	4			
	PoE Mini PC	8			
	PoE LED Troffer	8			
PSE 1	PoE Camera	4	13.7	28.7	74%[3]
PSE 1	PoE PAC	4	45.8	63.9	
PSE 5	PoE Mini PC	8	152.8	222.3	
PSE 5	PoE LED Troffer	8	619.6	813	

In contrast, decentralized systems suffer from redundant electrical energy usage due to internal computers of the switches, as each smaller switch introduces its own controller, resulting in a cumulative reduction in efficiency. This compounding effect makes centralized architectures a more efficient choice for large-scale deployments, particularly in environments with diverse power demands. The findings highlight the importance of selecting the appropriate system architecture to optimize PoE system efficiency, with centralized systems the preferred option when minimizing energy consumption is critical.

Next, the research team conducted a cybersecurity analysis, beginning with a review of product documentation from manufacturers referred to as PoE Manufacturer 1-9 in this report. In addition to assessing documentation for cybersecurity guidance, the team evaluated each device's compliance with relevant cybersecurity standards, including **California Senate Bill 327 (SB 327) Security of Connected Devices Law**, which mandates that IoT devices sold in California include reasonable security features such as unique passwords or the requirement to generate new credentials before initial access. The team also reviewed compliance with **UL/ANSI 2900: Software Cybersecurity for Network-Connectable Products**, a standard designed to evaluate networked products for vulnerabilities, malware, and the effectiveness of their software risk management processes. While SB 327 is required for devices sold in California, UL/ANSI 2900 is a voluntary standard that helps manufacturers demonstrate robust cybersecurity practices.

The documentation review revealed significant variations in the coverage of cybersecurity measures relating to installation and commissioning. While PoE requirements and network interface specifications were well-documented, there were notable gaps in cybersecurity guidance. Many documents lacked detailed instructions on secure installation practices, endpoint hardening, and network security configurations. Key aspects like changing default credentials, disabling unused services/ports, and firmware/software updates were inconsistently addressed.

The cybersecurity standards compliance evaluation further highlighted these shortcomings (Table 4). Several devices, such as those from PoE Manufacturer 3 and 7, were found to be non-compliant with both SB 327 and UL/ANSI 2900, lacking encryption, authentication, and update mechanisms. Devices like PoE Camera showed partial compliance, offering strong encryption but failing in areas such as password management and resilience to malformed inputs. PoE Manufacturer 8 and 9 devices demonstrated the strongest compliance, with PoE Manufacturer 8 fully meeting SB 327

---

[3] Weighted average

requirements and PoE PAC achieving full compliance with both standards. This analysis underscored the need for manufacturers to provide comprehensive cybersecurity guidance to ensure secure deployment of PoE systems, particularly in commercial environments where potential cyber threats could be significant.

Table 3. Summary of Cybersecurity Standards Compliance for PoE Devices

Device	SB 327	UL/ANSI 2900	Description
PoE LED Driver, PoE Mini PC, PoE USBC	Non-compliant	Non-compliant	No encryption or authentication mechanisms. Lacks firmware update features.
PoE Camera	Partial compliance	Partial compliance	Strong encryption but lacks unique preprogrammed passwords. Vulnerable to denial-of-service attacks due to failed malformed input tests. Outdated cryptography (MD5) and weak brute force protection.
PoE Shades	Non-compliant	Non-compliant	Relies on weak encryption, vulnerable to replay attacks, no authentication.
PoE AP	Compliant	Partial compliance	Strong encryption and secure authentication. Requires unique passwords at setup. Complies with SB 327 and UL/ANSI 2900 standards but some uncertainties in malformed input handling and logging. Cryptographic data storage supported, but specific key management undetermined.
PoE PAC	Compliant	Compliant	Comprehensive encryption and authentication, supports firmware updates.
PoE VAV Controller	Could not assess	Could not assess	Could not evaluate due to lack of communication over standard network protocols. Requires proprietary software for configuration. BACnet accessible, but only reports alarms and proprietary points.

Building on the standards compliance assessment, the research team carried out real-time penetration testing on multiple PoE systems, including a PoE lighting system and PoE shades, following manufacturer-recommended configurations. The testing revealed critical vulnerabilities in both systems. For the lighting system, the team identified risks related to unencrypted data transmission, insufficient authentication protocols, and inadequate switch security configurations. Techniques such as packet sniffing, command decoding, and MAC flooding were used to expose these flaws, demonstrating potential unauthorized control and data interception within the PoE system.

In the case of the PoE shades a critical vulnerability was discovered in the encryption protocol. While the system used a hashed message structure to authenticate commands, it failed to properly implement a counter value in the hash, making it susceptible to replay attacks. A replay attack occurs when an attacker captures valid data transmissions and replays them at a later time to trick the system into performing unauthorized actions. In this case, the research team captured traffic using a network tap between the Manufacturer 3 PoE controller and the shades. They were then able to manipulate the shades by replaying previously captured commands.

Additionally, the team explored other exploitation techniques, such as ARP spoofing, to intercept traffic and bypass network security measures. ARP spoofing (Address Resolution Protocol spoofing) is a method where an attacker sends falsified ARP messages on a local network, allowing them to impersonate legitimate devices by linking their MAC address to the IP address of another device. This can redirect network traffic to the attacker.

This vulnerability, combined with the relatively easy access to PoE cables in less secure areas, heightened the risk of attacks, particularly for publicly accessible devices. The research demonstrated how replay attacks could be executed using captured hash values for specific shade positions, completely bypassing the intended security mechanisms.

Introduction

The majority of building power distribution systems use alternating current (AC). This significantly influences the design of connected, building system components and appliances such as direct current (DC) appliances. With the proliferation of DC devices as standard design elements across many building technology categories, the interest in DC power distribution systems has also increased significantly. Power over Ethernet (PoE) leverages existing Information Technology (IT) infrastructure in the form of power switches, CAT cables and the IP protocol to facilitate communication and power distribution. Many control components across building systems are being designed with PoE compatibility to save energy on the AC-to-DC conversion, facilitate networking, and reduce installation cost.

The shift to centralized PoE architecture in building systems represents a significant change from traditional non-PoE network architectures. Traditional systems typically feature a single device connected to the IP network, transmitting data between the IP network and a downstream network, often proprietary. In contrast, the centralized PoE architecture uses a star topology, with every endpoint directly connected to the IP network. This architecture expands the IP threat surface compared with existing systems, increasing cyber vulnerabilities. Therefore, these systems require design considerations with a focus on security. Manufacturers should also educate customers and installers about these security implications when aggregating building systems onto a central PoE switch.

This report presents the findings of the ‘PoE Microgrid for Commercial Buildings Lab Evaluation’ project, focusing on evaluating the electrical efficiency and cybersecurity implications of utilizing PoE building systems, relative to traditional AC building systems. The project assesses the electrical efficiency of PoE-enabled building control components, such as VAVs, security systems, thin clients, and lighting, comparing them with their AC-powered equivalents. The evaluation includes designing two PoE Microgrid models: one using separate PoE switches for each building system, and another using a single PoE switch for all systems. The efficiency of these systems is compared with each other and to a conventional AC system.

The second aspect of this project is the cybersecurity assessment. The goal is to rigorously evaluate the cybersecurity measures recommended by each PoE system manufacturer, ensuring these align with current cybersecurity standards for networked building controls. This assessment involved a detailed analysis of the manufacturers' suggested installation and commissioning procedures, with an emphasis on identifying and addressing potential vulnerabilities in the network architecture.

Objectives

The objectives of the "PoE Microgrid for Commercial Buildings Lab Evaluation" project are:

- **Evaluate Electrical Efficiencies of PoE Devices vs AC Counterparts**: Assess the power consumption and overall system efficiency of PoE devices in comparison with AC-powered devices.
- **Evaluate Electrical Efficiencies of Centralized vs Decentralized PoE Systems**: Compare the efficiency of centralized PoE architectures to decentralized systems, focusing on how different configurations impact performance.
- **Evaluate Cybersecurity Documentation and Compliance:** Review the state of product documentation regarding cybersecurity measures for installation and commissioning, and assess device compliance with cybersecurity standards such as SB 327 and UL/ANSI 2900.

An integral part of the project is the design and evaluation of two distinct PoE Microgrid architectures. The first utilizes separate PoE switches for each building system, while the second architecture employs a single PoE switch to aggregate all systems. The efficiency of these systems was compared with each other but also against a conventional AC power distribution system to establish a comprehensive understanding of their operational efficiencies, compared with traditional AC technology.

The research team then conducted an in-depth evaluation of cybersecurity measures that are recommended by PoE system manufacturers. This included scrutinizing installation and commissioning procedures, assessing potential vulnerabilities in the network architecture, and evaluating these measures against the backdrop of current cybersecurity standards for networked building controls.

Methodology

Market Assessment of PoE Enabled Building Control Systems

The CLTC research team conducted an extensive market assessment of Power over Ethernet (PoE) building control technologies. This assessment covered both Powered Devices (PD) and Power Sourcing Equipment (PSE) and highlighted an increase in the breadth of PoE-enabled products across various building system categories.

The research team found that higher power PSE’s have entered the PoE market across a range of form factors (8 to 24 ports) to meet the increasing power requirements of advanced PoE-enabled devices. This trend is supported by advancements in PoE specifications, notably IEEE 802.3bt Type 4, which allows for power delivery of up to 90 watts per port. The increased power allotment has also led to the emergence of PoE devices across various markets, including lighting, HVAC, and IT devices, by meeting the need for increased power.

The market assessment revealed that many large lighting manufacturers are now offering PoE lighting solutions, while some PoE manufacturers have designed devices to retrofit existing LED luminaires into PoE-enabled luminaires. PoE's presence is also expanding within the IT sector, with a wide array of market-available PoE-enabled access points, thin clients, USB-C-powered devices, monitors, and more.

Furthermore, the assessment identified PoE-enabled devices across a broad spectrum of building system sectors including HVAC controllers, dynamic fenestration controllers/devices, physical access control systems, and security systems. This underscores the versatility and growing acceptance of PoE technology as part of modern building infrastructure.

Finally, the assessment noted the continued wide availability of PoE switches in various sizes, including different port numbers and power allotments. This variety is beneficial because matching the total PoE switch output to its expected load can lead to increased electrical efficiency. This comprehensive examination revealed a marked shift towards integrating PoE technology across multiple building control systems, highlighting its potential for streamlined power management and connectivity in building systems.

Technologies Evaluated

The technologies selected for evaluation were a cross-section of PoE-enabled building control devices identified during the market assessment. The products, encompassing both Powered Devices (PDs) and Power Sourcing Equipment (PSEs), varied in which PoE standard they employ, including IEEE 802.3af and IEEE 802.3bt Type 4 standards. For a baseline comparison, the research team also selected devices that utilize traditional AC power architecture.

POE SWITCHES

In the evaluation of PoE switches for microgrid applications, the research team analyzed a variety of switches from leading manufacturers. The study aimed to evaluate the performance, power output, and efficiency of various PoE switches under different loading scenarios. The selected devices included switches with varying maximum power capacity and functionalities, from Manufacturer 1 models that provide between 15.4-60W per port and Manufacturer 2 switch designed for medium to smaller scale applications, to Manufacturer 3 switches that provide 90W per port, capable of supporting larger loads like LED luminaires. Each switch was evaluated for its power delivery capacity and electrical efficiency under various loading conditions. Table 5 highlights some of the key specifications for the PoE switches selected for evaluation.

Table 4. PoE and Port Specifications For The Selected PoE Switches

Device	Max Output Power (W)	PoE Spec	Ports	Manufacturer
PSE 1	120	IEEE 802.3af, 802.3at	8 ports, 15.4-30W/port, 120W total	1
PSE 2	240	IEEE 802.3at, 802.3bt 3	8 ports, 30W/port	1
PSE 3	2,160	IEEE 802.3bt 4	24 ports, 90W/port	1
PSE 4	240	IEEE 802.3bt 3	8 ports, 30-60W/port, 240W total	2
PSE 5	720	IEEE 802.3bt 4	8 ports, 90W/port	3
PSE 6	2,160	IEEE 802.3bt 4	24 ports, 90W/port	3

Manufacturer 1

The research team selected three PoE switches from Manufacturer 1: PSE 1, PSE 2 and PSE 3. The PSE 1 supports IEEE 802.3at PoE+, IEEE 802.3af. It is capable of delivering up to 30W of power to any port with a total PoE power budget of 120W. This limitation means that, at maximum, only four ports can simultaneously supply 30W, due to the overall power budget constraints.

The PSE 2 model was selected for evaluation because of its higher power output capabilities. The PSE 2 Switch has eight ports with 2.5GE data transfer speeds and includes dual 10G copper/SFP+ combinations for uplink connections. It features a total PoE power budget of 240W, supporting both 802.3at and 802.3bt Type 3 configurations across its ports. However, it restricts the allotment of 60W per port to only four ports at a time to manage the overall power budget. By default, these ports are limited to 30W, but the device allows for manual configuration via the command line interface to enable the full 60W on four ports.

The PSE 3 is a larger, 24-port switch that is distinguished by its use of the IEEE 802.3bt Type 4 protocol, which allows for a power delivery of up to 90W per port. To achieve the higher power output, the switch can be equipped with a secondary 1900W power supply, upgrading from the original single 1100W unit. With the upgraded power supplies, the PoE budget is substantially increased to 2160W, enabling each of the 24 ports to deliver the full 90W. This higher power switch was key to the study, as it presented the best potential for achieving the highest energy efficiency due to its high capacity. This significantly expanded the ability of the research team to test a wide variety of PDs, enhancing the assessment of PoE technologies' efficiency and capability in supporting numerous high-demand devices within PoE microgrid applications.

Manufacturer 2

The PSE 4 is a medium scale PoE switch with a maximum power output of 240W. It supports IEEE 802.3bt 3 (PoE++) on ports 1 to 4 with a power output of 60W each. Additionally, ports 5 through 8 are compatible with IEEE 802.3at (PoE+), each providing 30W. This model was identified during the market assessment as being well suited for PoE IT and Physical Access Control (PAC) applications, given its capacity for 30-60W power delivery. According to the product documentation, the first four ports are specifically optimized for high-bandwidth devices such as 2.5G PCs, PTZ (pan-tilt-zoom) cameras, and WiFi 6 access points, while the latter four are tailored for IP cameras, and less power-intensive access points and routing devices.

Manufacturer 3

Similar to the PSE 3 switch, the PSE 5 switch was selected for this study because it can deliver 90W per port, the highest power allotment available for current PoE technology, while having only eight ports. This made it representative of a switch that might be used to power the lighting system for a room or a few offices, rather than larger, more extensive installations. Its 720W total power capacity and smaller port count make it ideal for scenarios requiring high power output on a limited number of devices, such as LED luminaires, without the need for larger, more complex switches.

The research team evaluated a 24-port high power capacity switch, the PSE 6. This switch is capable of a PoE power output of 2.16kW and supports up to 90W per port. This capacity allows it to power a broad range of devices, essential for applications such as lighting and security systems within a network. With twenty-four 10/100/1000Base-T Ethernet PoE ports, the switch enables efficient power management and distribution. The switch also offers gigabit transmission speeds for Ethernet uplink ports and SFP slots, providing a comprehensive solution for network efficiency and connectivity.

POE POWERED DEVICES

The PoE system evaluation involved the analysis of a diverse range of PoE-enabled building devices. These devices were carefully selected to cover a broad range of power requirements and encompass multiple building systems such as lighting, computing, access control, and automated window treatments.

The selected devices represented the breath of technologies and power demands typical in modern building automation environments. Table 6 describes the selected products and details some of their key PoE related specifications.

Table 5. Selected PoE Technologies

Device	PoE Spec	Description	Manufacturer	Building System
PoE LED Driver	IEEE 802.3bt 4	LED driver, 4-Channel Driver, 90W max	3	Lighting
PoE Mini PC adapter	IEEE 802.3bt	PoE adapter for Mini PC	3	IT
PoE USB-C	IEEE 802.3bt 4	USB Power and Data Supply	3	IT
PoE AP	IEEE 802.3af	WiFi Access Point	8	IT
PoE PAC	IEEE 802.3bt	Access control system	9	Physical Access Control
PoE Shades	IEEE 802.3af/at	PoE enabled roller shades	7	Lighting
PoE VAV Controller	IEEE 802.3af	VAV controller for HVAC	6	HVAC
PoE Camera	IEEE 802.3af	Networked Security Camera	5	Physical Access Control

Manufacturer 3 PoE System

The research team selected the PoE Manufacturer 3 system for evaluation due to support capabilities with respect to a wide array of PoE-enabled building systems including lighting, computing, and USB-C charging applications.

The PoE LED Driver follows the IEEE 802.3bt Type 4 standard and is capable of driving up to four LED fixtures with a combined power consumption of 90W. It is fully configurable via the PoE controller software and can be set up for either constant current (CC) or constant voltage (CV) power delivery. The PoE LED Driver can integrate with various sensors such as occupancy, illuminance, and daylight sensors.

The PoE Mini PC adapter enables PoE capability for Mini PCs from, providing up to 60W of power directly to the Mini PC through a single Ethernet connection. Within this evaluation, the PoE Mini PC adapter represented a medium-load IT PoE device.

The PoE USB-C Docking Station operates on the IEEE 802.3bt Type 4 standard, requiring up to 90W and capable of delivering a continuous USB-C power of 72W and data delivery to devices like smartphones, tablets and laptops, supporting additional peripherals like keyboards and storage devices. The PoE USB-C Docking Station demonstrates the PoE system's capability to support diverse end-user devices and applications within building systems.

PoE Camera

The next PD selected for evaluation by the research team was the PoE networked security camera. This device requires IEEE 802.3af PoE or 12V DC power input with a maximum power consumption of 12W. IP cameras are commonly PoE-enabled for ease of installation, so this device was selected to assess the electrical efficiency of powering such devices through the PoE system. With a 12W power draw per camera, it is well-suited to fully load the smallest IEEE 802.3af PoE switches, which provide up to 15.4W per port.

PoE VAV Controller

The next selected PD was the PoE VAV Controller. This device is a BACnet Advanced Application Controller designed for VAV applications. It operates on both IEEE 802.3at PoE (25.5W max) and 802.3af PoE (12.95W max) standards. The controller can also provide 24V DC power output to external field devices rated at 16.8W (700mA) for 802.3at or 7.2W (300mA) for 802.3af. Its PoE compatibility and ability to power other devices were key factors evaluated to assess the system's capability to integrate and efficiently power VAV controllers and associated peripherals within building automation networks.

PoE Shades

The PoE motorized window shades were selected for evaluation as a lighting/automated fenestration system component. These shades are designed to operate on IEEE 802.3af/at PoE, requiring up to 15.4 watts of power. Accordingly, they are compatible with any standard PoE switch or injector. The PoE shades were selected to demonstrate the breadth of available PoE building technologies.

PoE AP

The PoE wireless access point represents a PoE-enabled IT device. It supports IEEE 802.3af Power over Ethernet with a maximum power consumption of 15.4W, allowing it to be powered directly from most PoE switches and injectors. Access points are a common PoE-enabled device in modern building networks. Its inclusion provides insights into the electrical efficiencies associated with powering IT devices via PoE instead of traditional AC adapters.

PoE PAC

The PoE PAC devices were evaluated as PoE-powered access control devices. The Access Hub operates on IEEE 802.3bt Type 3 with a maximum power draw of 51W, enabling it to be powered from any switch supporting this standard and to provide power to accessory devices such as with two Access Readers and one Protect camera. The door access scanner is powered via PoE from the access hub and requires up to 6W. Evaluating PoE-enabled access control hardware provided valuable insights into powering security and entry management systems efficiently through the PoE building infrastructure.

COMPARABLE AC/DC TECHNOLOGIES

To assess the electrical efficiencies of PoE-enabled building control devices, the research team procured equivalent devices powered by 120V AC to serve as the baseline for product comparisons (Table 7).

Table 6. Comparable AC Technologies

Device	Description	Manufacturer	Building System
LED Luminaire Driver	1 Channel Driver, 40W max	AC Manufacturer 1	Lighting
Mini PC	Small windows PC	AC Manufacturer 2	IT
USB Charger/Laptop Charger	USB Power and DC Laptop Charger	AC Manufacturer 3	IT
AP*[4]	WiFi Access Point	PoE Manufacturer 8	IT
AC PAC	Smart locking system	AC Manufacturer 4	PAC
Shade*	Controllable shading system	PoE Manufacturer 7	Lighting
VAV Controller*	VAV controller for HVAC	PoE Manufacturer 6	HVAC
Camera*	Networked Security Camera	PoE Manufacturer 5	PAC

Devices that were equipped with both PoE and AC/DC adapter inputs, such as the PoE Camera and PoE AP, were ideal for this comparison. These devices were evaluated under both power conditions using the same units to minimize measurement variation caused by manufacturing or electrical variances possible across multiple products of the same type. Additionally, some devices the team tested served as PoE adapters for non-native PoE devices. For example, one device was designed to power an Mini PC via PoE, even though the Mini PC is typically powered by an AC/DC wall adapter. This PoE adapter accepts a PoE input and outputs DC power through a barrel jack, while also providing data through a CAT 5 cable. The baseline efficiency for these devices was established by measuring the electrical power consumption when powered by the manufacturer's supplied AC-to-DC wall adapter. For products available in distinct PoE and AC versions, like the PoE VAV Controller and PoE Shades, both product variants were tested.

For certain devices such as the PoE LED Driver and the PoE PAC controller, where directly comparable PoE and non-PoE models did not exist, alternative devices were selected for evaluation. Alternatives were matched against closely related PoE products in terms of power consumption, functionality, and features. For the PoE LED Driver an AC-powered LED driver were evaluated. For the PoE PAC, a similarly featured AC/DC-powered access control system was selected.

---

[4] * designates that the AC version of the device is the same as the PoE device i,e, the device has two power inputs.

Electrical Analysis

Test Equipment

The research team used three different power analyzers to quantify the electrical efficiencies of the selected technologies. These meters, all produced by Xitron, include models XT2640AH and XT2640AX (Figure 4), and the Xitron 2802 (Figure 5). Despite their similar appearances, the XT2640AX model is designed to measure current with external CTs (Current Transformer), whereas the XT2640AH model measures current with an inline shunt resistor. The Xitron 2802 model is a two-channel device that measures voltage and current similarly to the XT2640 and was used to measure AC power for this experiment. Both XT2640 models are equipped with four channels, allowing for simultaneous measurement of multiple devices. Data is collection from the XT2640AH and XT2640AX through an external USB drive, while the Xitron 2802 model interfaces with a data collection terminal PC for data acquisition purposes.

Figure 2: Metering Equipment: Xitron XT2640AH (left) and the Xitron XT2640AX (right). Data acquisition terminal (PC) in the rear of the two meters.

Figure 3: Xitron 2802 used for inline measurement.

The current transformers (CTs) used in this study were Fluke i30s which are AC/DC Hall-effect clamp style CTs. These CTs were positioned around the conductors carrying current, as shown in Figure 5, with the measurements being displayed on the Xitron AX meters. The following table compares the three Xitron meters and the specifications:

Table 7: Xitron Meters Characteristics

	Xitron 2802	Xitron Xt2640AX	Xitron XT2640AH
Measurement Type	Current Transducer / In-Line	Current Transducer	In-Line
Voltage Range	850 Vrms	External voltage output CT or Shunt Input (20µV to 15Vrms) with resolution down to 0.1µ	N/A
Current Range	10Arms	N/A	High Current (up to 30Arms continuous and 200Apk in rush) with resolution down to 10µA, also capable of being used with a current output CT.
Accuracy	0.005%	0.005%	0.005%
Element Type	N/A	26A Element	
No Damage Current Range	N/A	8ms< : <200Vrms and <300Vpk	8ms < : <200Arms and <300Apk
	N/A	40ms< : <50Vrms	40ms< : <75Arms
	N/A	1s< : <30Vrms	1s< : <50Arms
	N/A	Continuous: <25Vrms to Vpeak	Continuous: <30Arms
Nominal Dimensions	119.4mmH x 350mmW x 241mmD	137mmH x 248mmW x 284mmD	

	Xitron 2802	Xitron Xt2640AX	Xitron XT2640AH
Nominal Weight	3.4kg	3.2kg	

Each Fluke CT was securely mounted on a measurement platform, designed to hold the CT in a fixed orientation during measurements (Figure 6). PoE standards, including IEEE 802.3af/at and bt, feature variations like Mode A and Mode B, which specify how power and data are delivered across different wire pairs within Ethernet cables, accommodating various power consumption levels. Depending on the PoE standard used, a given wire pair may carry positive current or negative current. This measurement platform also ensured that the Fluke CTs was oriented in the correct direction relative to the current flow which is important according to the manufacturer. Furthermore, the measurement platform enabled the research team to accurately capture voltage readings on the appropriate power carrying conductor.

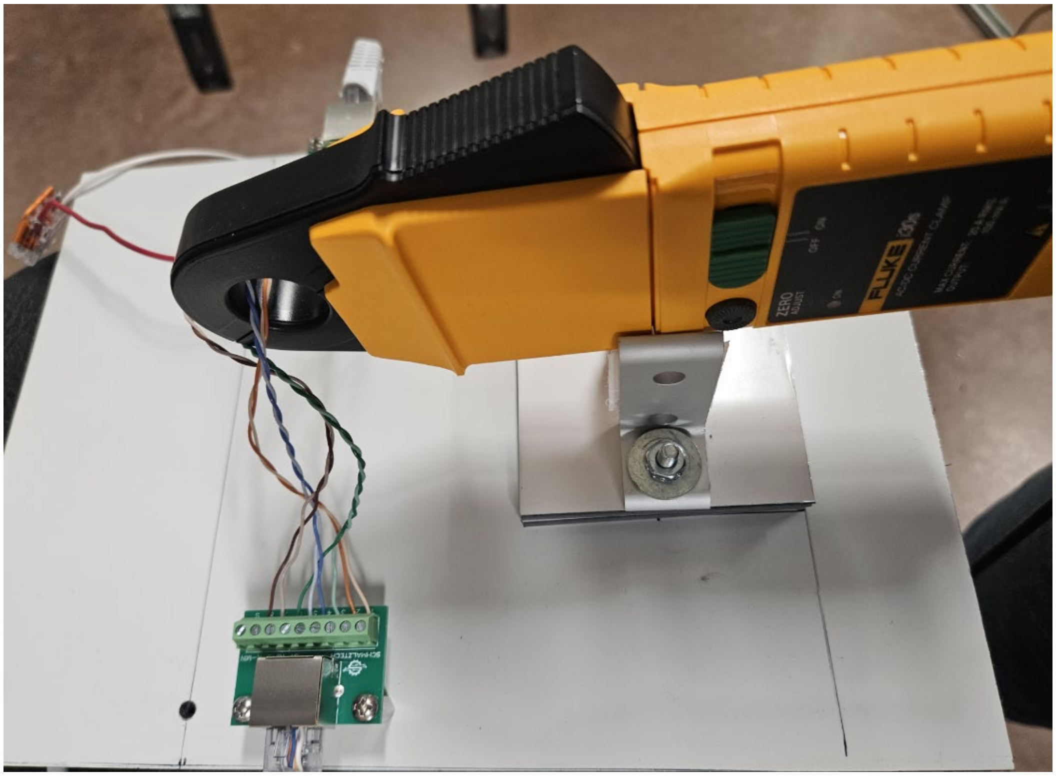

Figure 4: Fluke CT with Ethernet cable conductors passed through.

Experimental Approach

This evaluation utilized three distinct measurement configurations tailored to the electrical architecture of the devices and referred to as ‘Configuration 1, 2 and 3’. The primary objective was to characterize the electrical efficiency of each power-consuming device/module within the system's architecture. For every device, electrical measurements were taken before (M1) and after (M2) the PoE switch. For certain PoE devices, like the PoE Camera and PoE AP, these measurements represent the full extent of possible data collection, as the CAT cable providing PoE power ends at the device (Figure 7). For these PoE devices with fully integrated/internal PoE-to-usable DC conversion circuitry, quantifying the power losses of the PoE-to-DC conversion process is not feasible without a comprehensive understanding of the device's internal design and circuitry. While measurements can be taken at the input to PoE-to-DC circuitry, tracing the power beyond that point and pinpointing the losses within the device itself becomes challenging without access to detailed schematics.

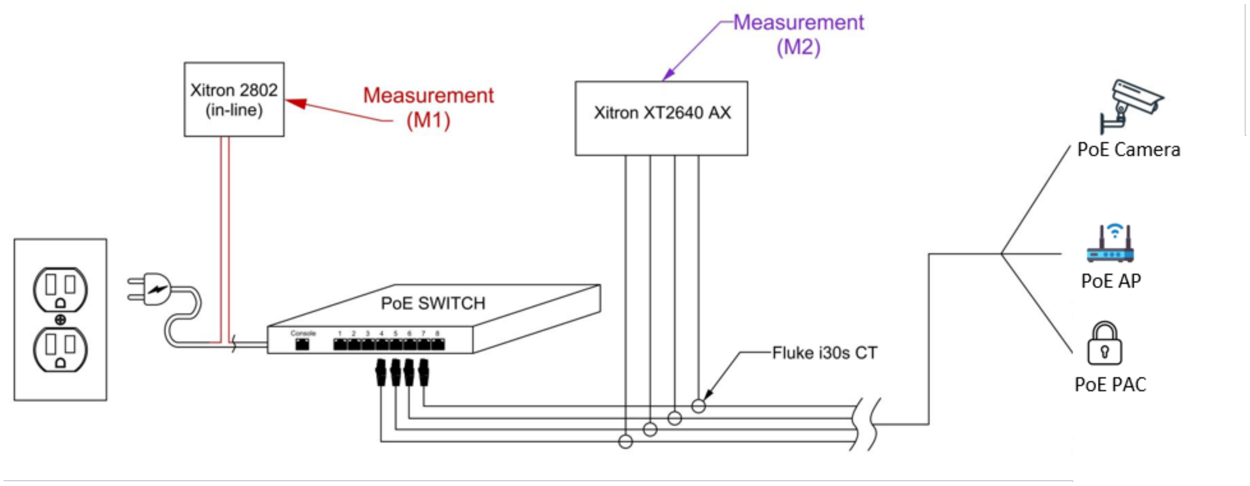

Figure 5: Measurement configuration 1 for PoE Camera, PoE PAC and PoE Wireless Access Point

For other devices such as the PoE LED Driver and PoE Mini PC adapter, voltage and current measurements were collected after the PoE node, just before the load (M3). Only two of the six selected PoE switches were used to power each PoE end point at the time of this report. For each experiment, either four or eight PoE devices were connected to the switch, depending on the test, but due to metering equipment limitations, only up to four devices were directly metered. Specifically, in scenarios where eight devices, such as PoE LED Driver and PoE Mini PC adapter, were connected, the remaining four unmetered devices were assumed to perform similarly to the metered devices. For all test, the devices were connected to the PoE switches with equal length CAT5e cables and allowed to stabilize before commencing a one-hour data collection period with one-minute sampling intervals.

For Configuration 1, voltage and inline current measurements were taken with a Xitron 2802 between the wall plug providing mains power and the PoE switch (M1). This measurement captures the total power consumption by the PoE system. The second current and voltage measurement (M2) was taken after the switch but just before the PoE end point using a Xitron XT2640-AX with a Fluke i30s CT clamp meter. The Fluke i30s current transformer was used since the current carrying conductors in the CAT cables also carry data. For this evaluation, all current measurements on CAT cables were done using these Fluke i30 CTs in conjunction with the Xitron XT2640-AX meter.

The total system efficiency for this configuration is defined in equation 1.

$$Total\ System\ Efficiency_1\ (\%) = \frac{Measurement\ (M2)}{Measurement\ (M1)} \times (100) \qquad (1)$$

Configuration 2 is similar to the first configuration but has an additional measurement point (M3) after the PoE device but before the load (Figure 8). For devices such as the PoE LED Driver and PoE Mini PC adapter, it is possible to measure the DC power delivered directly to the device after the PoE node. This additional measurement point (M3) allowed the team to quantify the efficiency of the PoE nodes themselves, providing a more complete characterization of the PoE system efficiency.

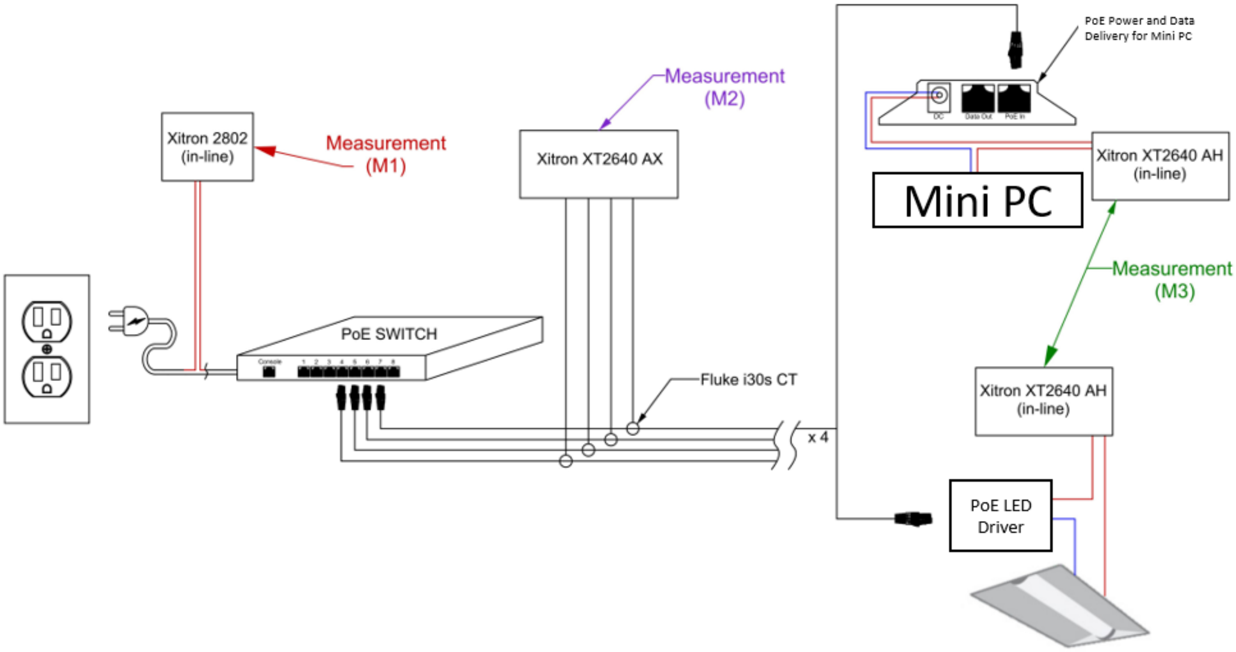

Figure 6: Measurement scheme 2 for the PoE Mini PC and the PoE LED Luminaires.

The PoE Mini PC adapter accepts PoE power through a “PoE In” port and outputs DC power through a barrel jack “DC Out” port directly to the Mini PC barrel jack power port. The PoE Mini PC adapter similarly has a “Data Out” Ethernet port that provides the IP data to the Mini PC’s Ethernet port. The PoE LED driver takes PoE power and data at its input and has four constant current/voltage DC outputs intended to drive LED luminaires. For both of these devices, voltage and inline current measurements (M3) were taken using a Xitron XT2640-AH. For this measurement scheme, M1 and M2 remain the same as the previous scheme.

The total system efficiency, switch efficiency and the node efficiency for this second scheme can be calculated using the following equations:

$$Total\ System\ Efficiency_2\ \ (\%) = \frac{Measurement\ (M3)}{Measurement\ (M1)} \times (100) \tag{2}$$

$$Switch\ Efficiency(\%) = \frac{Measurement(M2)}{Measurment(M1)} \times (100) \tag{3}$$

$$Node\ Efficiency\ (\%) = \frac{Measurement\ (M3)}{Measurement(M2)} \times (100) \tag{4}$$

A third measurement configuration using the Xitron XT2640AX was used to establish the baseline efficiencies of the traditional non-PoE AC devices. In Configuration 3, all current measurements were inline. AC Current and voltage are measured before the AC power adapter similar to M1 in the previous configurations. DC voltage and inline current measurements were taken with a Xitron XT2640-AH after the AC/DC power brick but just before the device itself (Figure 9).

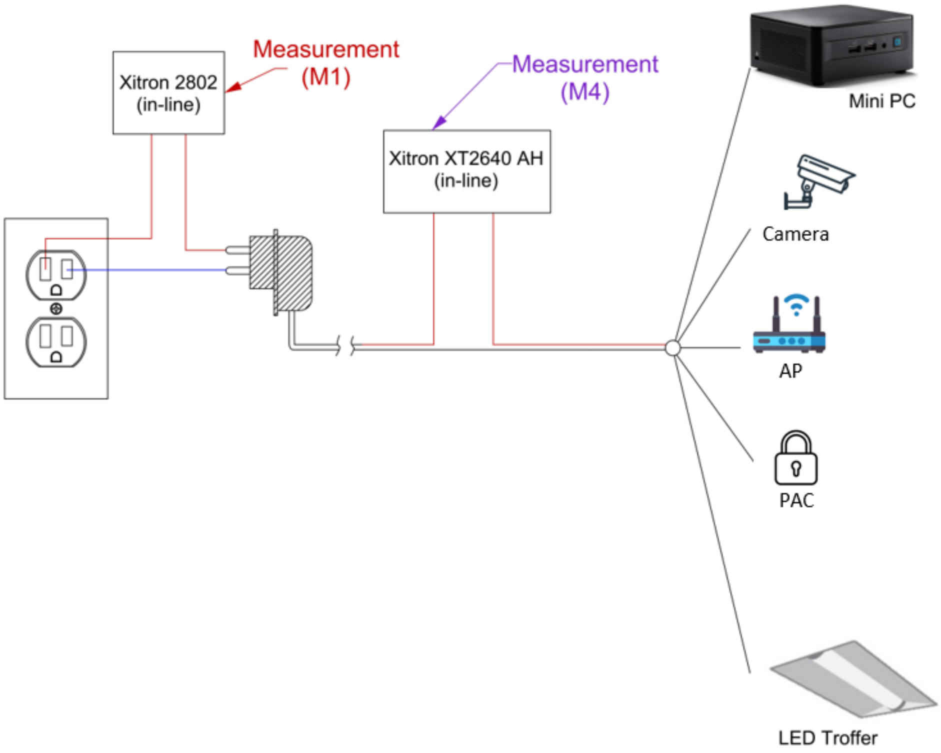

Figure 7: Measurement scheme 3 for the power adapters/bricks for each device.

The efficiency of the AC power supply is calculated using the following equation:

$$Power\ Supply\ Efficiency\ (\%) = \frac{Measurement\ (M4), P_{DC}}{Measurement\ (M1), P_{AC}} \times 100 \qquad (4)$$

The actual laboratory setup is shown in the Figure 10. The devices are mounted on strut for the ease of measurement. Each of the devices can be connected to the switch rack with a designated CAT5e cable that are all of equal length to ensure consistent test conditions between devices.

Figure 8: Rail mounted devices.

The PoE switches evaluated in this study were mounted in a network rack that was centrally located in the PoE Microgrid lab. The PSE 5 and PSE 6 switch are notable in that they both require rack-mounted power supply unit(s), distinguishing it from the other switches with integrated supplies. The central location of the PoE switch rack and the bundles of labeled, equal length cables, made it easy for the research team to connect any PoE end point to any of the switches.

Cybersecurity Analysis

Review of Product Documentation

The cybersecurity analysis began with a comprehensive literature review of the product documentation provided by the PoE system manufacturers. This review focused on evaluating both the cybersecurity measures recommended by the system manufacturers for system installation and configuration, as well as the devices' compliance with relevant cybersecurity standards, such as SB 327 and UL/ANSI 2900. While the documentation review provided insight into the manufacturers' guidance, the evaluation of compliance with cybersecurity standards required hands-on testing of the devices. This testing involved assessing key features like encryption, authentication mechanisms, and resistance to exploits such as brute force attacks or malformed inputs. The guidance from manufacturers varied widely, from detailed instructions on hardening endpoints within the system to more general advisories such as "consult your IT department for proper network configuration." This stage aimed to collate and assess all such recommendations, in the following categories:

- Device overview/specifications

- Recommended installation procedures
- Specific endpoint security measures (e.g., firmware updates, access controls)
- Network controls and configurations on the PoE switch (e.g., VLAN segmentation, encrypted standards)
- Compliance with relevant cybersecurity standards
- Recommended PoE switch configurations (e.g., port security, DHCP snooping)

Real Time Cybersecurity Analysis/Penetration Testing

The next step involves a two-phase real-time cybersecurity analysis and penetration testing of each PoE system:

- **Phase 1: Manufacturer's recommendations configuration:** In this phase, the switch and connected PoE systems are configured strictly according to the manufacturer's recommendations. This configuration serves as a baseline to assess the security of the system as dictated by the manufacturer.
- **Phase 2: Industry standard configuration:** In the second phase, the switch and systems are reconfigured according to the cybersecurity standards identified by the research team as most relevant and robust for these types of systems.

During both phases, the research team conducted penetration testing to uncover any potential vulnerabilities such as use of unsecure protocols, unauthorized access, injection attacks (such as SQL injection and cross-site scripting), man-in-the-middle (MitM) attacks, and firmware vulnerabilities.

The penetration testing adhered to the following approach:

1. **Vulnerability scanning and reconnaissance**
    - This initial stage involved scanning the network and systems to identify all connected devices, their configurations, and potential vulnerabilities. This step was crucial for mapping out the network and understanding the possible entry points for cyber attacks.
2. **Simulating attacks**
    - Following the reconnaissance, simulated cyber attacks were carried out. This phase tested the system's resilience to various attack vectors, such as network intrusions, session hijackings, or other forms of unauthorized access attempts.
3. **Exploitation of vulnerabilities**
    - If vulnerabilities were identified during the attack simulations, the next step was to attempt to exploit these weaknesses. This stage assessed the potential damage or control that could be gained by exploiting identified security gaps. For building control systems relying on unencrypted network protocols, common exploitation methods could involve sniffing network traffic to capture sensitive data, conducting man-in-

the-middle attacks to intercept and modify communications, or exploiting weaknesses in authentication mechanisms to gain unauthorized access or send malicious commands.

4. **Post-exploit control and assessment**
    - Once a vulnerability is successfully exploited, this phase evaluated the level of control or access gained. It assessed the impact of the exploit on the system's integrity, data confidentiality, and overall network security.

Each phase of this testing process provided valuable insights into the security posture of the PoE systems. It identified specific areas where security enhancements are needed and helped in understanding the effectiveness of manufacturer recommendations versus industry-standard configurations.

Results

Electrical Analysis

The following sections provide a comparative analysis of the electrical efficiencies for each selected PoE technology. This analysis was conducted by powering PoE endpoints using the PSE 5 and PSE 2 PoE switches and comparing the results to those obtained when the devices were powered by their traditional AC wall adapters. The goal was to assess the electrical efficiency of using PoE switches relative to conventional AC power sources. Additionally, these sections detail the findings from an experiment that measured the total system efficiency of a consolidated PoE microgrid. This test was carried out using both a PSE 6 switch and a PSE 3 switch. The efficiencies of these consolidated microgrids were then compared to those of a decentralized architecture, where the same devices were powered by individual PoE switches selected to match their output capacity to the specific load required by each device. In the decentralized architecture, each smaller switch was dedicated to powering only one type of PoE device, effectively segmenting different PoE devices from one another.

PoE vs. AC system efficiencies

POE CAMERA

To evaluate the electrical performance of the PoE cameras, two separate tests were conducted. In the first test, electrical measurements were taken with the cameras connected to the PSE 5 switch, and in the second test, the same measurements were repeated with the cameras connected to the PSE 2 switch. For both tests, CAT 5e cables were used to connect the cameras, which were allowed to operate in their default/unconfigured state. The electrical measurements were taken per 'Configuration 1' as previously described, wherein electrical meters were connected both upstream of the PoE switch and immediately preceding the PoE camera's input (Figure 12).

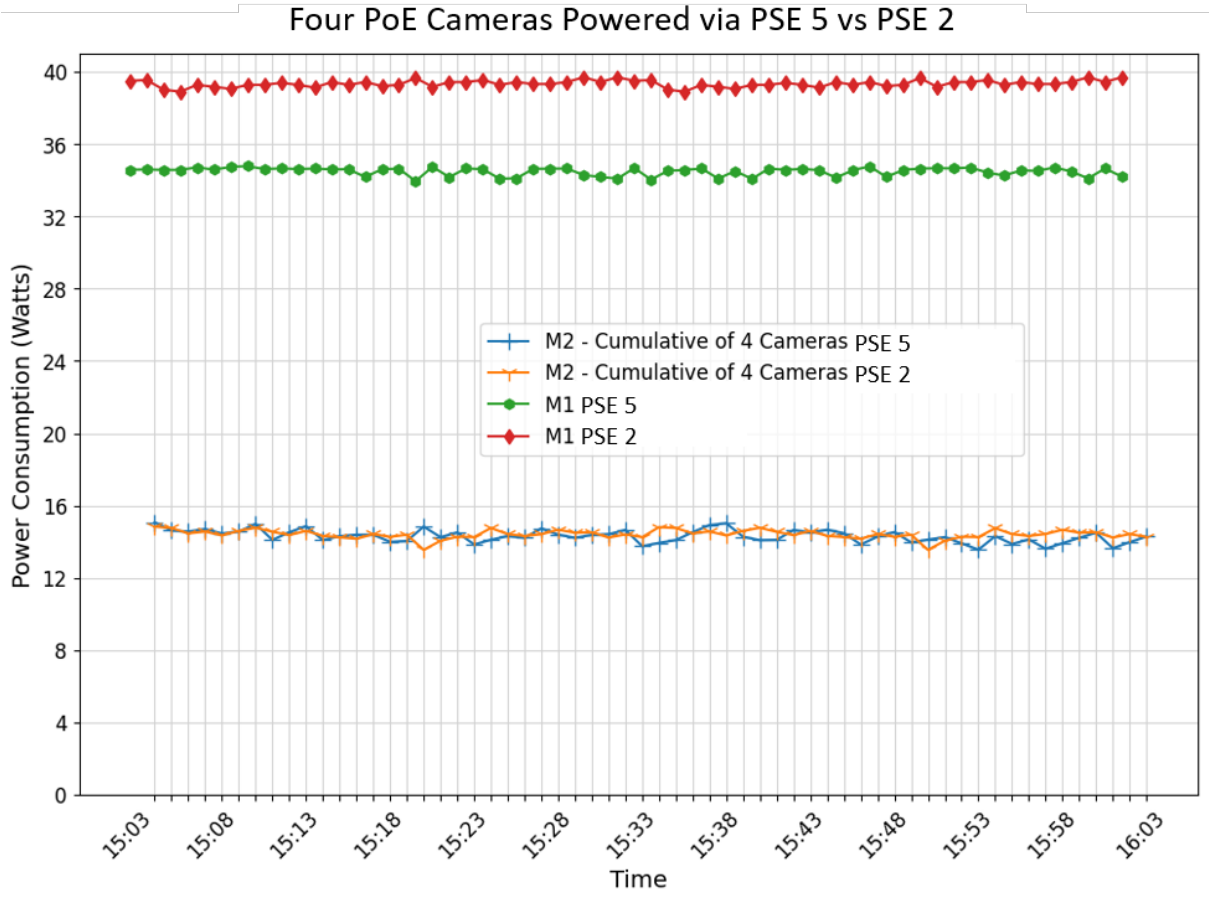

Figure 9: The total power consumption of four PoE Cameras on PSE 5 vs PSE 2.

For both the PSE 5 and PSE 2 PoE switches as power sources, the PoE cameras each drew an average 3.5W with a total power consumption for all four cameras of 14.31W when powered by the PSE 5 and 14.41W when power by the PSE 2 switch. However, the total system power consumption when powered by the PSE 2 switch was about 5 Watts higher than when powered by the PSE 5, suggesting that the PSE 2 switch itself requires more power under these loading conditions. Specifically, the PSE 5 switch drew 34.49W while the PSE 2 switch drew 39.34W from the A/C source even though they both provided nearly identical power to each of the four cameras. The total system efficiency of the PoE switch and PoE cameras was calculated using Equation 1 and was found to be 41 percent when using the PSE 5 switch, compared with 37 percent when using the PSE 2 switch (Table 9).

Table 8: PoE Cameras on PSE 5 vs PSE 2

	PoE Cameras		
	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency[1] (%)
PSE 5	14.31	34.49	41%
PSE 2	14.41	39.34	37%

Next, the research team evaluated the power consumption of the AC/DC version of the Camera. Since the Camera can be powered either via PoE or DC via an RJ45 and barrel jack port respectively, the same camera was used in the AC/DC evaluation. The research team procured a 12V, 1A AC-to-DC power supply based on the rated power requirements of the camera. At the time of writing, Camera Manufacturer (Manufacturer 5) does not offer an AC-to-DC power supply for this device. The power supply was metered per Configuration 3 for a total of one hour with a one-minute measurement interval (Figure 13).

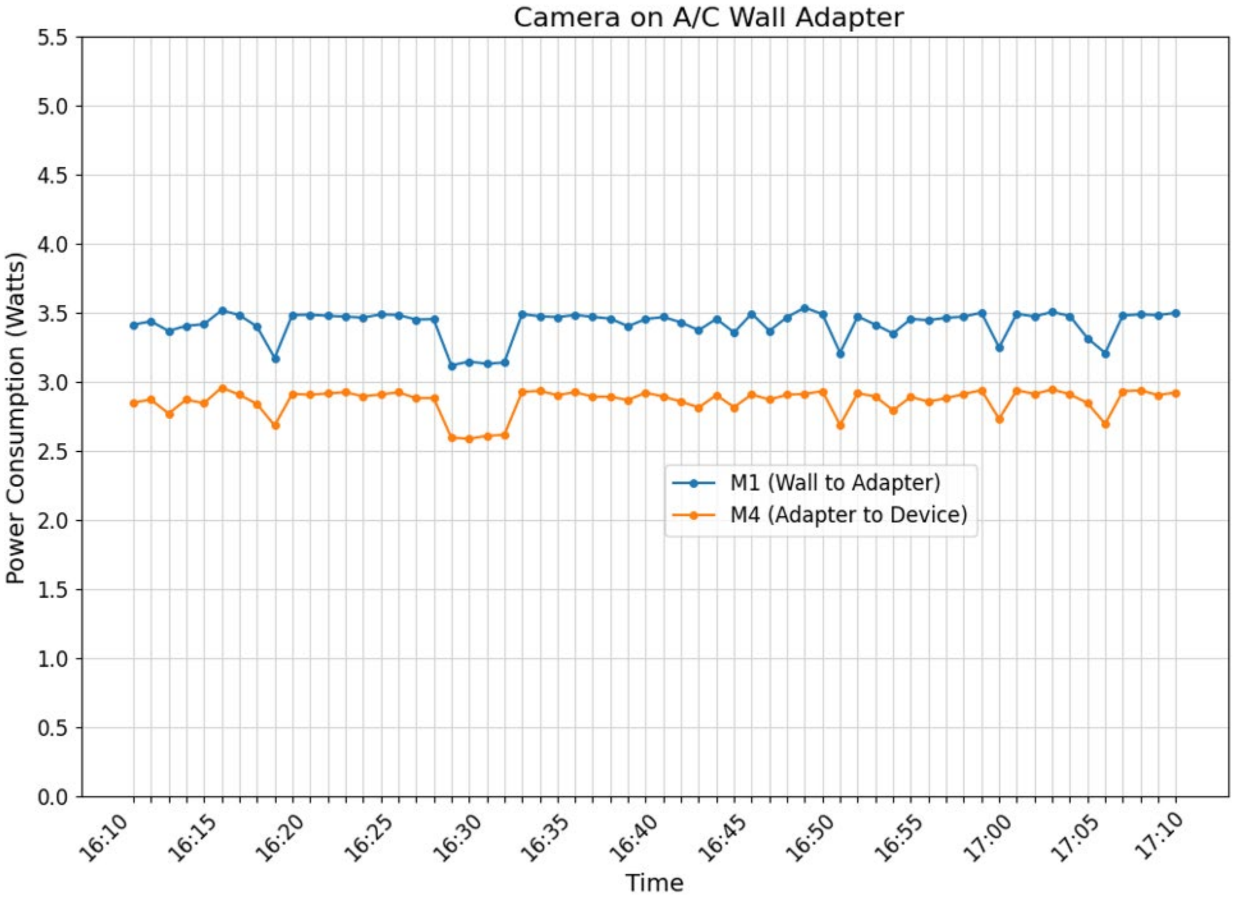

Figure 10: A/C adapter power consumption for camera

When powered from an AC wall adapter, the camera drew less power than when powered by either PoE switch with an average of 2.86W (as compared to 3.5W). The research team speculated that the higher power draw when powered via PoE is due to the losses in the circuitry that converts the PoE power to usable DC within the camera. The AC-DC wall adapter for a single camera drew 3.42W from the wall receptacle and delivered 2.86W to the device itself, resulting in a power supply efficiency of 84 percent (Table 10).

Table 9: Power Consumption of the AC Adapter for the Camera

	Camera		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power Adapter	2.86	3.42	84%

This system efficiency was significantly higher than that of the PoE variant using PSE 5 and the PSE 2 switches, which had measured efficiencies ranging from 37 percent to 41 percent. For the PoE tests, the lower efficiencies observed can partially be attributed to the substantial power consumption of the PoE switch itself, which is significant compared to the 3.5W consumption of each camera. This additional power consumption greatly reduces the overall system efficiency.

POE WIRELESS ACCESS POINT

To evaluate the power consumption of the WiFi access points, two sets of tests were conducted. In the first set, four Access Point devices were connected to the PSE 2 PoE switch, and electrical measurements were collected. CAT 5e cables were used to connect the access points in their default/unconfigured state.

As seen in Figure 14, the cumulative power consumption of the fouraccess points (M2) averaged 18.79W, while the total system power consumption (M1) when powered by the PSE 2 switch averaged 46.95W. The significant difference between the power consumption of the access points and the system's total power draw indicates that the PSE 2 switch itself consumes a substantial amount of power, similar to the earlier findings with the cameras.

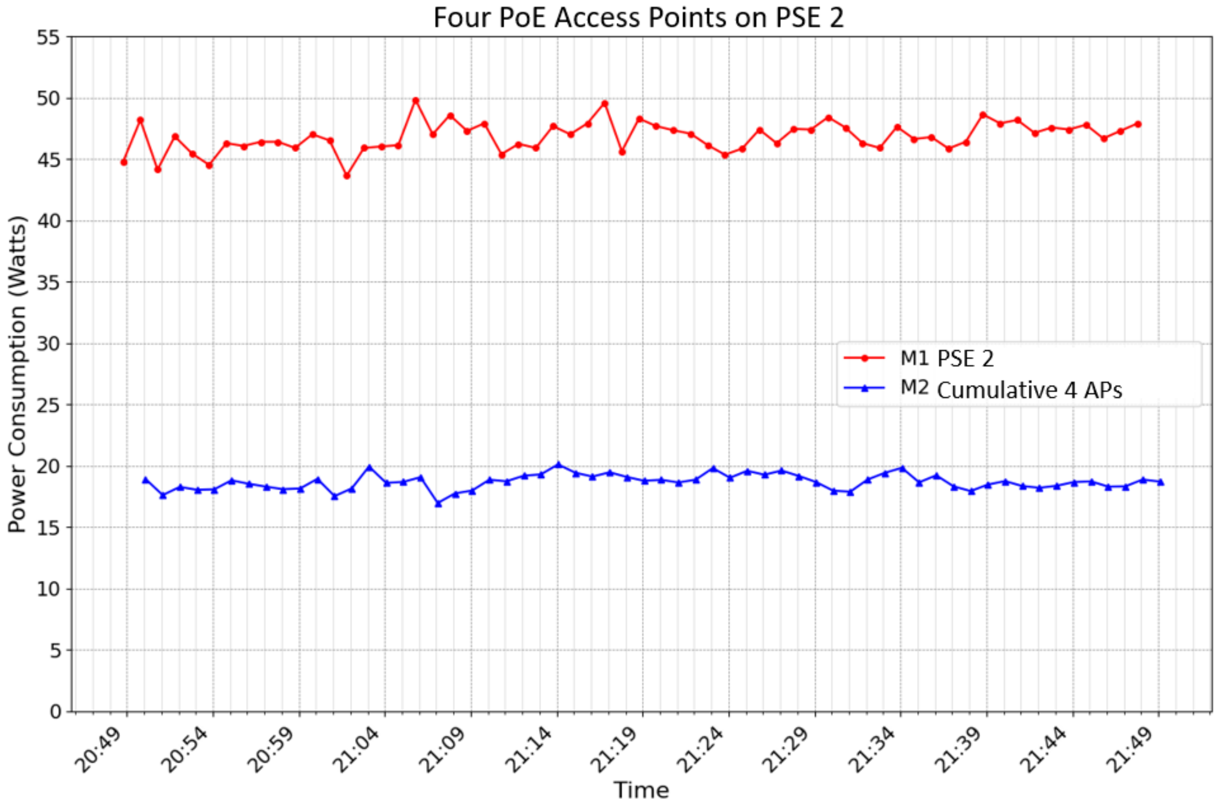

Figure 11. Total PoE power consumption of the Access Points when powered by the PSE 2.

The system efficiency, calculated using Equation 1, was determined to be 40 percent for the Access Point devices when connected to the PSE 2 PoE switch (Table 11). This lower efficiency can be attributed to the high baseline power consumption of the PoE switch, relative to the power consumed by the access points.

Table 10. PoE Access Point System Efficiency

	PoE Access Point		
	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency[1] (%)
PSE 2	18.79	46.95	40%

The next test evaluated the power consumption of the Access Point when powered using a 12V, 1A AC-to-DC adapter, as the device can operate through both PoE and DC inputs. Electrical measurements were taken per 'Configuration 3' over a one-hour period with one-minute intervals. As shown in Figure 15, the power consumption of an access point when powered via the AC adapter averaged 3.75W. The total power draw from the wall outlet to the adapter was measured at 4.35W. This resulted in a power supply efficiency of 87 percent (Table 12), which is considerably higher than the system efficiency observed in the PoE tests.

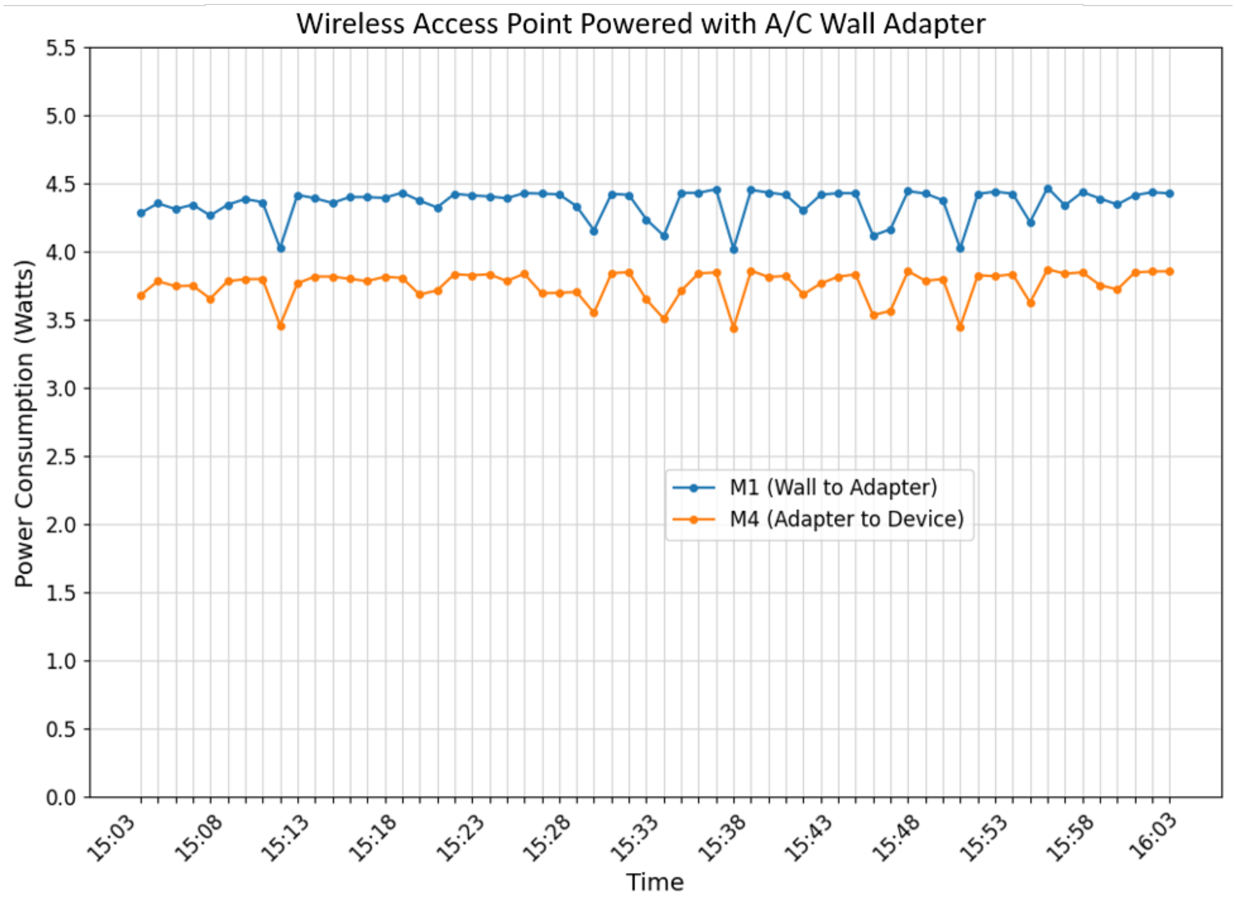

Figure 12. Power consumption of the Access Point when powered by AC.

The higher efficiency of the AC/DC adapter setup compared to the PoE system is consistent with previous findings, where the additional power required by the PoE switch reduces overall system efficiency. Furthermore, the reduced power conversion losses in the AC/DC adapter contribute to its superior efficiency (Table 12).

Table 11. System Efficiency of Access Point When Powered by AC

	Access Point		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power Adapter	3.75	4.35	87%

POE VAV CONTROLLER

The PoE VaV Controller was tested to evaluate its power consumption when powered by the PSE 2 PoE switch. As in previous tests, CAT 5e cables were used to connect the controller to the switch, and electrical measurements were taken per 'Configuration 1,' with meters installed both upstream of the PoE switch and directly before the controller's power input.

The cumulative power consumption of two PoE VaV controllers (M2) was measured at an average of 31.39W, while the total system power consumption (M1), which includes the PSE 2 switch, was recorded at 48.34W (Figure 16). This indicates that, although the controllers consumed a moderate amount of power, the switch added a considerable overhead, leading to a lower system efficiency.

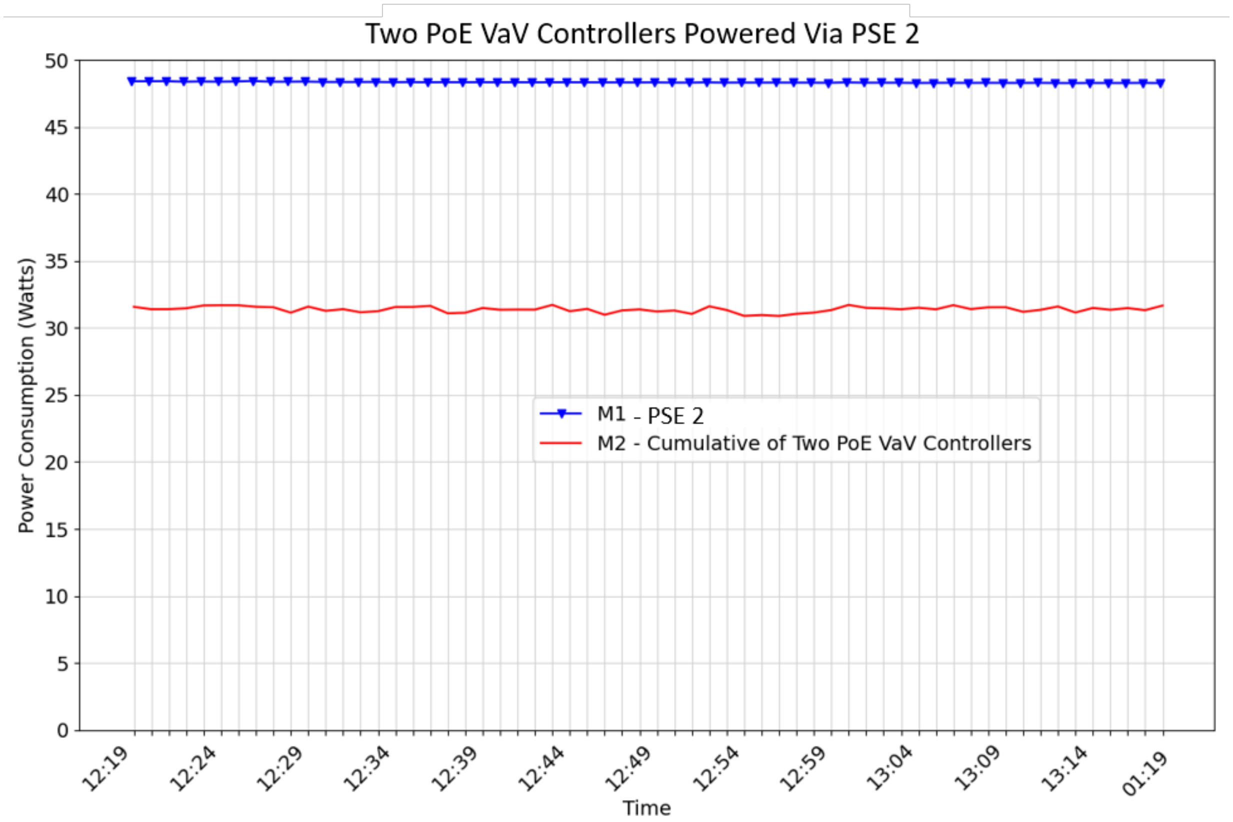

Figure 13. PoE power consumption of the PoE VAV Controller

The system efficiency for this configuration was calculated as 65 percent using Equation 1 (Table 13). This efficiency is higher than what was observed for some of the other PoE-powered devices, likely due to the relatively higher power consumption of the controllers, relative to other devices tested, which reduces the proportion of power lost to the baseline consumption of the switch.

Table 12. System Efficiency for the PoE VaV Controller when Powered by PoE

	PoE VaV Controller		
	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency[1] (%)
PSE 2	31.39	48.34	65%

The second set of tests measured the power consumption of the VaV controller when powered via an AC-to-DC adapter. The controller, which can be powered using either PoE or DC, was connected to a 12V, 1A AC power supply, with measurements taken per 'Configuration 3' over a one-hour period.

As depicted in Figure 17, the controller consumed an average of 13.09W when powered by the AC adapter. The total power draw from the wall to the adapter was measured at 15.13W, resulting in a power supply efficiency of 87 percent (Table 14). This efficiency is higher than the 65 percent observed when the controller was powered via PoE, indicating that the AC-to-DC power supply introduces fewer conversion losses and operates more efficiently than the PoE system.

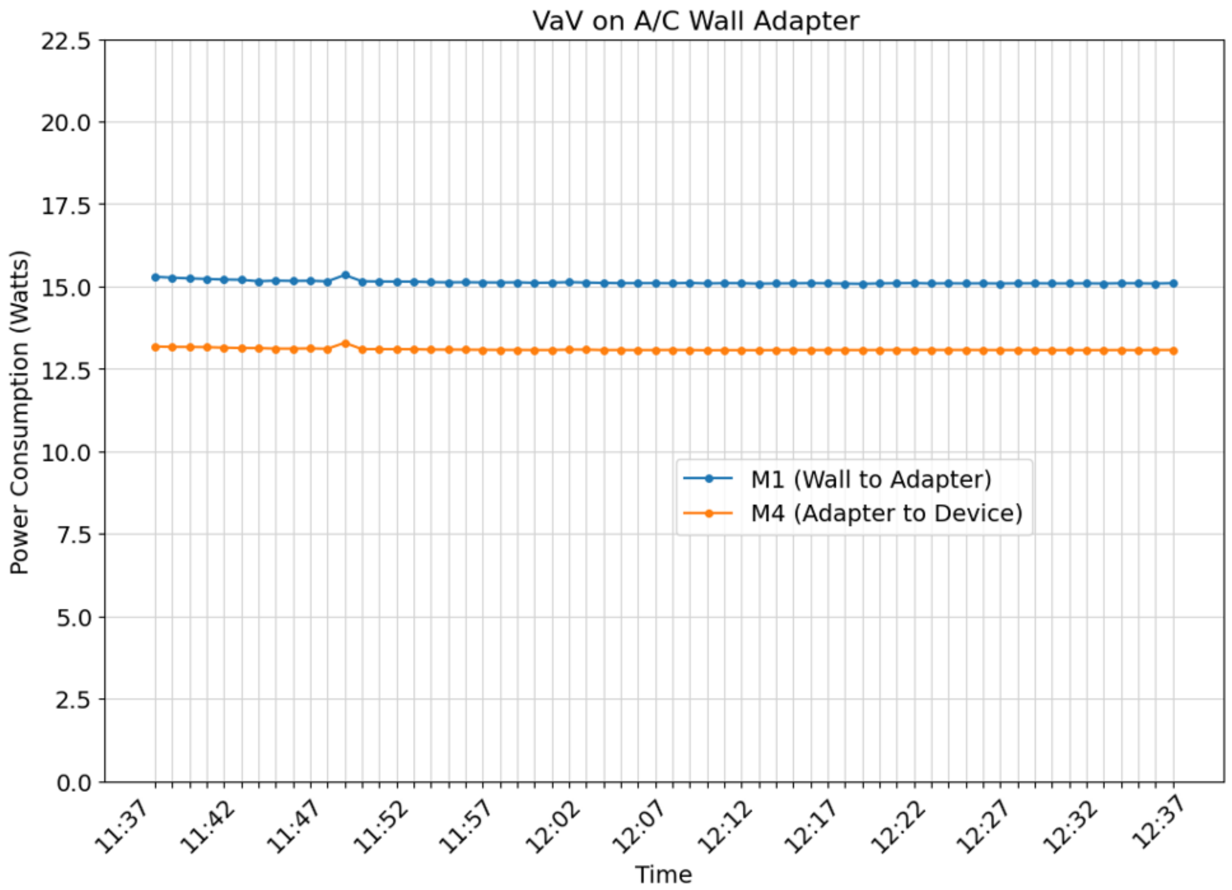

Figure 14. Power consumption of VaV Controller when powered by AC

The higher efficiency of the AC/DC adapter setup further reinforces the finding that PoE switches contribute significant overhead power consumption, particularly in configurations where the powered devices have relatively low power requirements.

Table 13. System efficiency of VaV Controller when powered by AC

VaV on A/C Wall Adapter			
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power Adapter	13.09	15.13	87%

POE SHADES

Next, the research team tested the PoE Shades to compare their electrical performance when powered by PoE, versus a standard AC/DC adapter. Two tests were conducted: one with the shades powered by a PSE 5 PoE switch and another using an AC power adapter to evaluate the differences in power consumption and overall system efficiency. During the PoE test, the cumulative power consumption of the three PoE Shades was measured, and the PSE 5 switch's overall power consumption was also tracked (Figure 18).

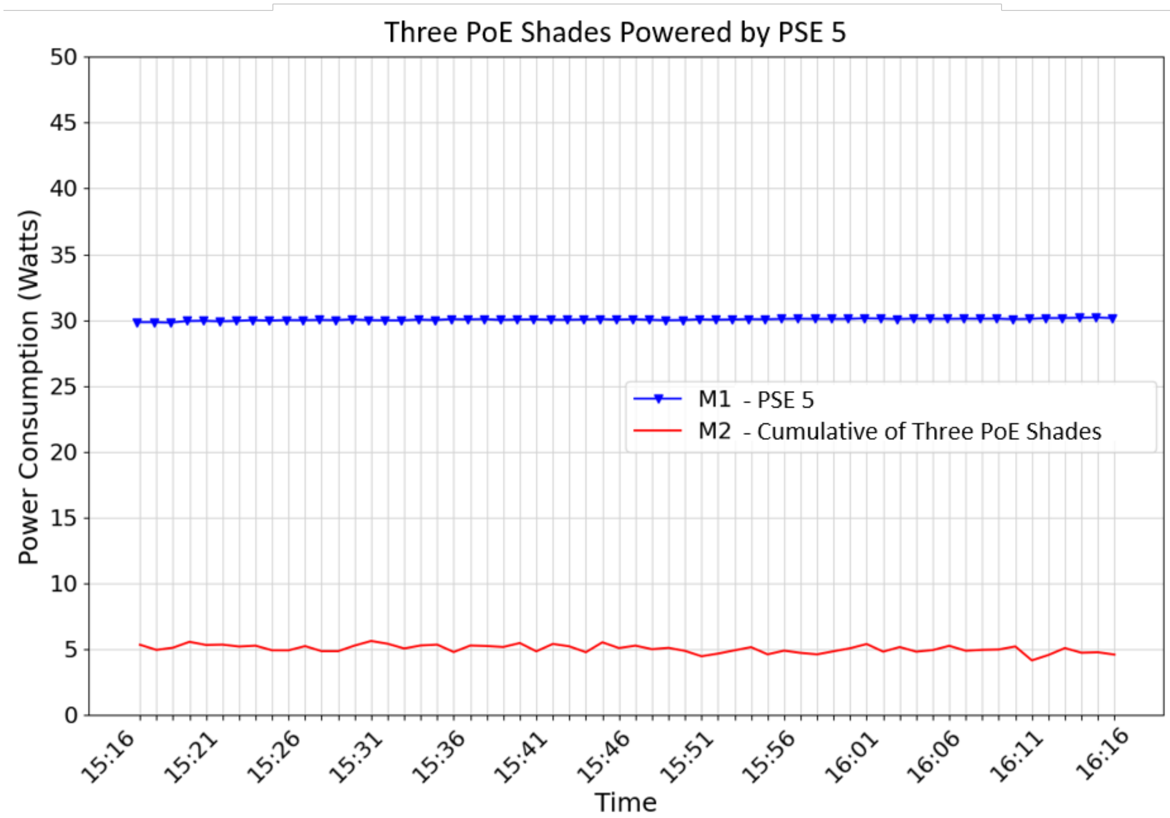

Figure 15. Power consumption of the PoE shades powered by PoE

The total power consumption of the three PoE Shades was 5.04W, or 1.68W each, while the PSE 5 switch consumed 30.05W, resulting in a system efficiency of only 17 percent (Table 15).

Table 14. PoE Shades System Efficiency

	PoE Shades		
	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency (%)
PSE 5	5.04	30.05	17%

In the AC/DC test (Figure 19), the Shades drew significantly less power. When powered by the AC adapter, the shades consumed 0.073W, while the adapter itself drew 0.11W from the wall, leading to a power supply efficiency of 67 percent (Table 16).

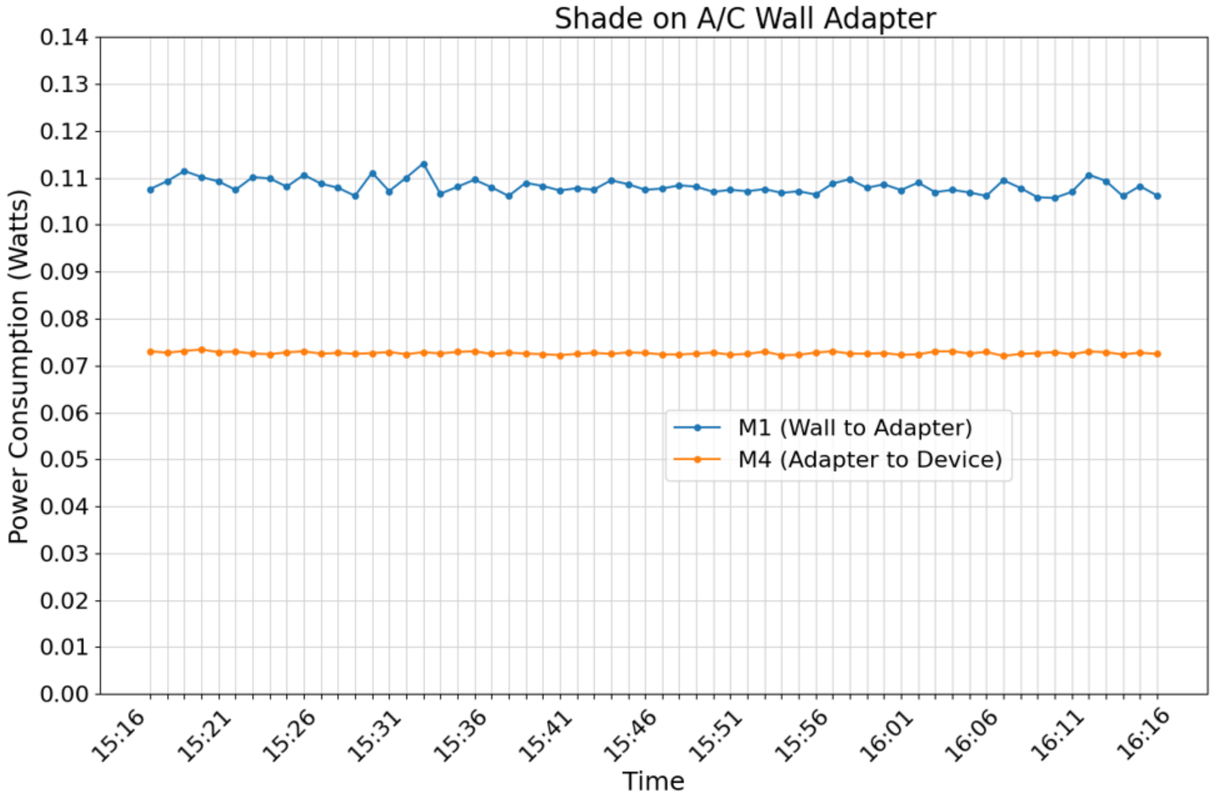

Figure 16. Power consumption of Shades when powered by AC

Upon closer analysis, the team discovered that the PoE version of the shades includes an internal battery and charging circuit, which the AC version lacks. This extra circuitry likely explains the increased power draw in the PoE configuration. Additionally, the relatively high--power consumption of the PoE switch itself, compared with the low draw of the shades, contributed to the low overall system efficiency in the PoE configuration. Consequently, this difference in hardware features between the PoE and AC versions means that the comparison between the two power sources is not directly equivalent, as the PoE version inherently uses more power for additional functions like battery charging.

Table 15. Shades System Efficiency when Powered by AC

	Shade		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power Adapter	0.11	0.073	67%

POE USBC

The power consumption of four USB-C controllers was evaluated using the PSE 4 PoE switch as the power supply. The controllers were connected using CAT 5e cables, with power draw measured per

'Configuration 1.' Meters were placed both upstream of the PoE switch and just before the controllers' input to measure the total system and device power consumption.

As shown in Figure 20, the cumulative power consumption of the four USB-C controllers (M2) averaged 218W, while the total system power consumption (M1), including the PSE 4 switch, was measured at 230W. This indicates that the PoE switch added a relatively small overhead to the system's total power draw.

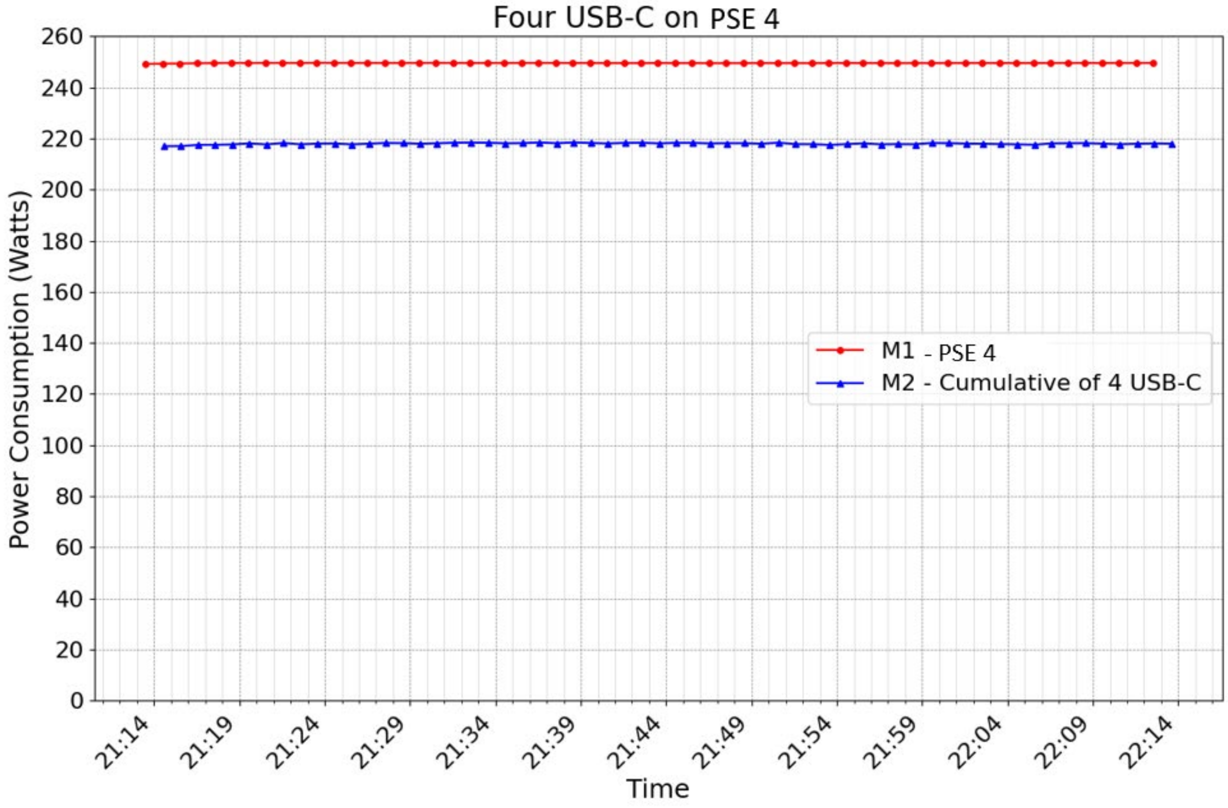

Figure 17. Power consumption of USBC controller when powered by PoE

The overall system efficiency was calculated to be 95 percent (Table 17), which is significantly higher than the efficiency observed for other devices powered through PoE. This high efficiency is primarily due to the substantial power draw of the USB-C controllers relative to the switch's own power consumption, leading to a lower proportion of power lost in the system.

Table 16. System Efficiency of USBC Controller when Powered by PoE

	USB-C		
	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency (%)
PSE 4	218	230	95%

In the second test, the USB-C controller was powered using a 12V, 1A AC-to-DC adapter, with measurements collected over a one-hour period.

Figure 21 shows the power consumption results from this configuration, with the controller drawing an average of 60.81W (M4) from the adapter. The total power draw from the wall outlet to the adapter was measured at 70.30W (M1), resulting in a power supply efficiency of 86.5 percent (Table 18). Although this is slightly lower than the PoE efficiency, it still represents a relatively efficient system for powering the device via AC.

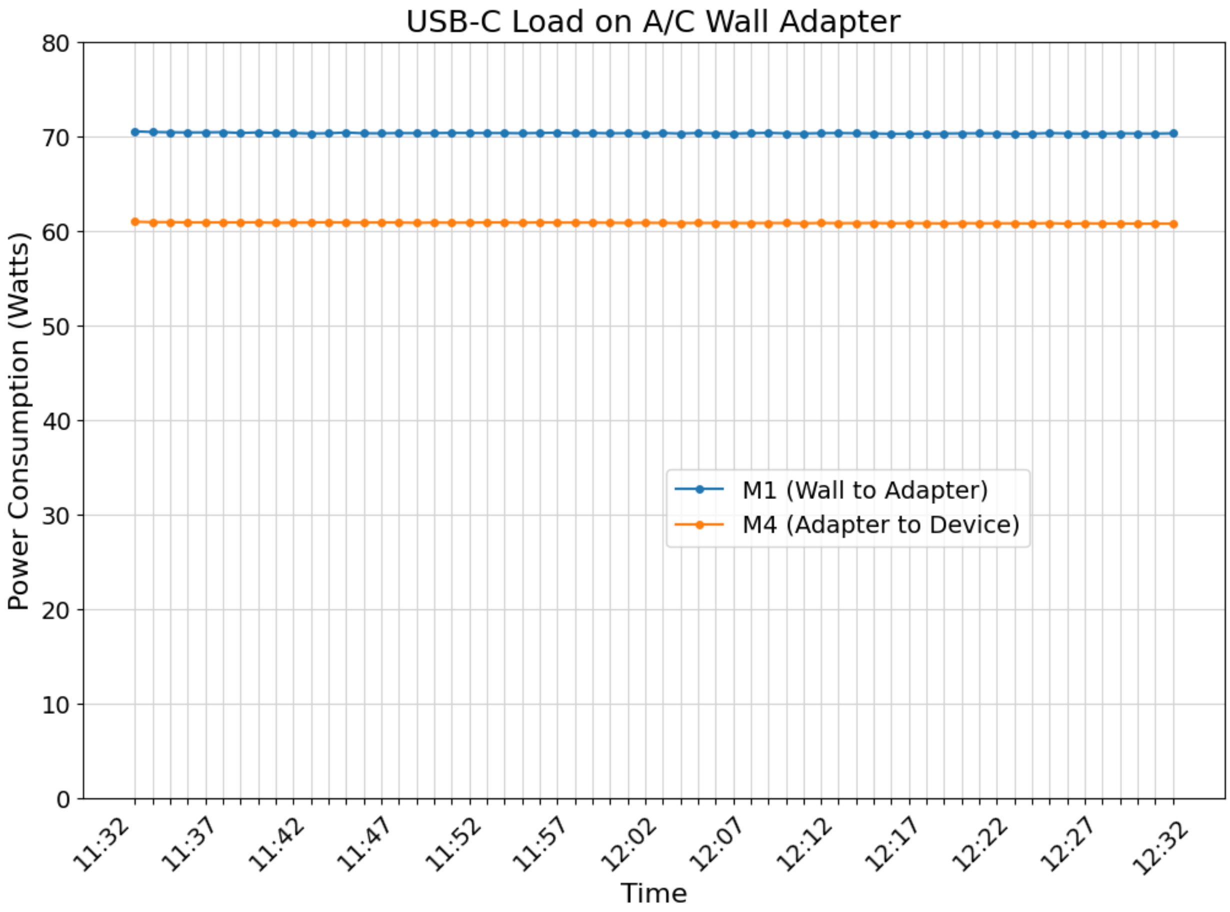

Figure 18. Power consumption of USBC controller when powered by AC

The comparison between PoE and AC power supply methods demonstrates that both approaches yield high efficiencies for the USB-C controllers, though PoE shows a marginally better system efficiency. The relatively high-power consumption of the USB-C devices compared with other tested systems minimizes the impact of switch or adapter overhead, leading to more favorable efficiency results overall.

Table 17. System Efficiency of USBC Controller when Powered by AC

	USB-C		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power Adapter	60.81	70.30	86.5%

POE ACCESS CONTROLLER

The Physical Access Controller was metered per Configuration 1 with the card reader and one 12W magnetic door locked attached to the hub as loads. The manufacturer specified that the card reader can consume up to 6W and the dry contact relay can handle a maximum load of 12W, equivalent to 12VDC at 1A. The research team loaded both the PSE 5 switch and the PSE 2 each with 4 Access Hubs, card readerss and magnetic door locks in their default/idle state for testing. The research team the measured electrical performance of the four access controllers connected to the PSE 5 and the PSE 2 switch, over a period of one hour (Figure 22).

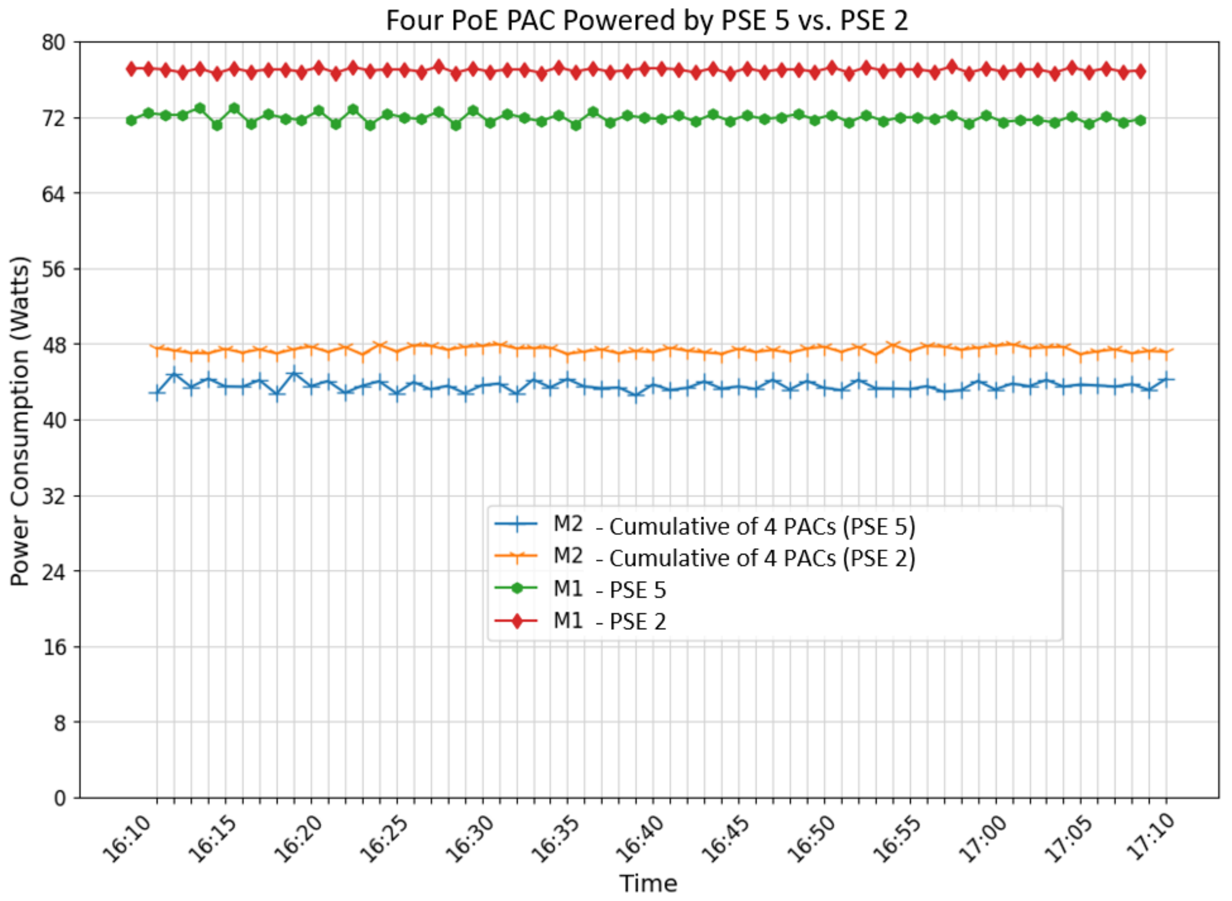

Figure 19: Total power consumption of four PoE Access Controllers on PSE 5 vs PSE 2

The electrical measurements collected for the Physical Access Controller showed that the devices consumed between 10.8-11.8W depending on which PoE switch was used to power them. When powered by the PSE 2, the total system power consumption was measured to be 77W as compared with 72W when powered by the PSE 5. Under these loading conditions, powering the access controllers with the PSE 2 switch resulted in a slightly higher total system efficiency by one percent, compared with using the PSE 5 switch (Table 19).

Table 18: Power Consumption of Physical Access Controller on PSE 5ort vs PSE 2

	Physical Access Controller		
	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency[1] (%)
PSE 5	43.55	71.93	61%
PSE 2	47.39	76.98	62%

The total system efficiency when powering the Physical Access Controller with the PSE 5 and the PSE 2 was calculated to be 61 percent and 62 percent, respectively.

Since the Physical Access Controller can only be powered with via PoE, an equivalent access control system was evaluated as a comparable AC variant. The AC PAC was selected due to its similar feature set, rated power consumption (60W max) and networking capabilities. For this test, the AC PAC was also powering/controlling the same magnetic lock and its own NFC credential card reader. Under these operational conditions, the average power consumption of the AC PAC was found to be 7.57W over the 1 hour test period (Figure 23).

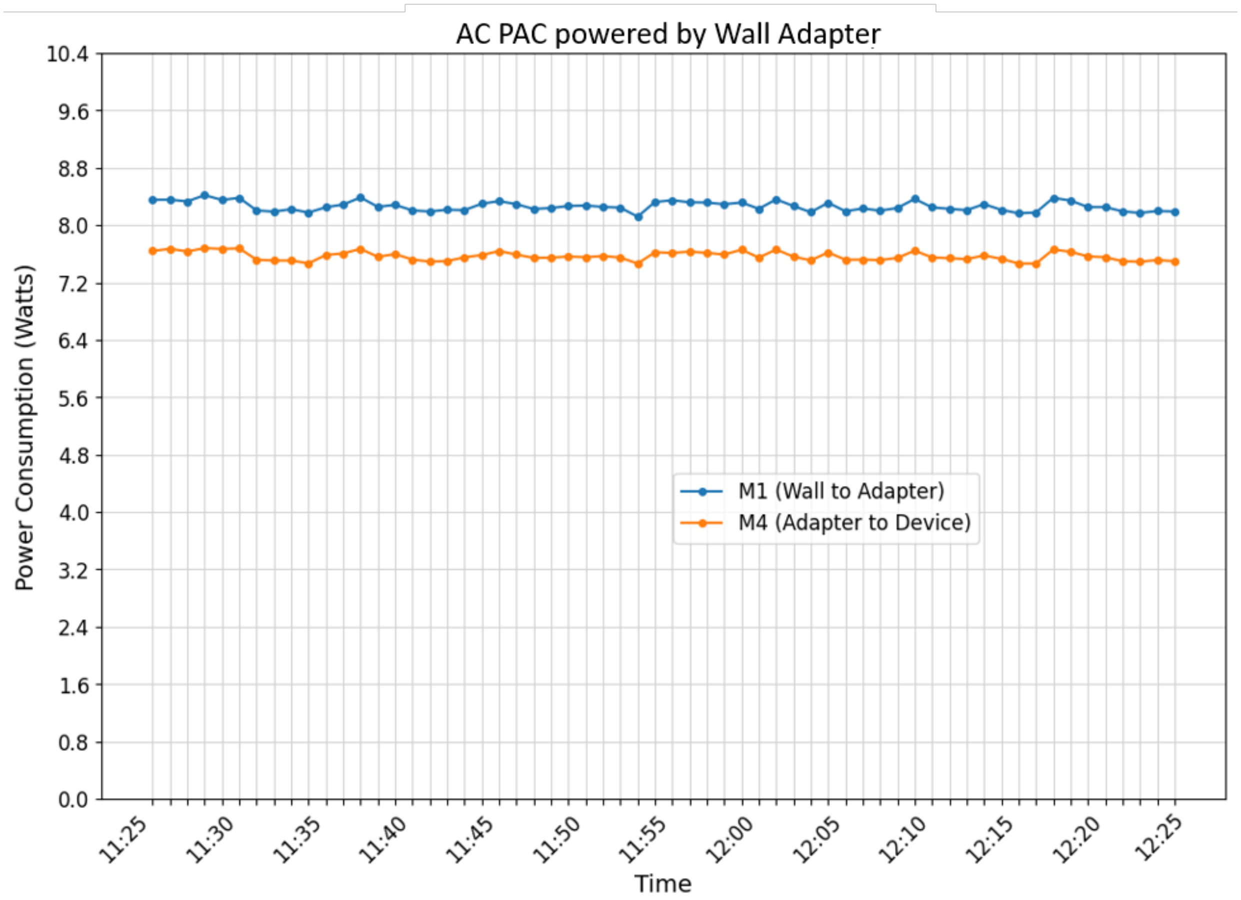

Figure 20: AC PAC Powered by AC Wall Adapter

As with the previous AC devices, the system efficiency refers to the electrical efficiency of the power supply. In the case of the AC PAC, the device is shipped with a AC/DC power adapter that is rated at 60W (24V, 2.5A). When tested with the same methodology as previously discussed power adapter achieved an efficiency of 92% (Table 20).

Table 19: Power Consumption of the AC Adapter for the AC PAC

	AC Physical Access Controller		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power	7.57	8.26	92%

POE MINI PC ADAPTER

The research team evaluated the electrical efficiencies of PoE Mini PC adapter when powered by both the PSE 5 and PSE 2 PoE switches. Capable of drawing up to 60 watts, the PoE Mini PC adapter represented the highest electrical load tested thus far. In contrast to earlier tests involving only 4 devices, for this evaluation, the team acquired 8 Mini PCs along with PoE Mini PC adapters. This was done to test the load capacity of the IEEE 802.3bt Type 3 and 4 switches. The PSE 5 switch can supply PoE power to the PoE Mini PC adapter without requiring any setup. In contrast, the PSE 2 switch requires configuration to activate four-pair power, enabling its maximum power output of 60W. The PSE 2 was only capable of powering 4 of the PoE Mini PC adapters as only 4 of its ports support the IEEE 802.3bt Type 3 standard. For all tests involving the Mini PC, a program was installed on each PC that forces the CPU to operate at 100% capacity thereby increasing the electrical load of the PC. For the test with the PSE 5 switch as the power supply, the Mini PCs with fully loaded CPUs only drew 18.5W on average, and 146.7W cumulatively (Figure 24)

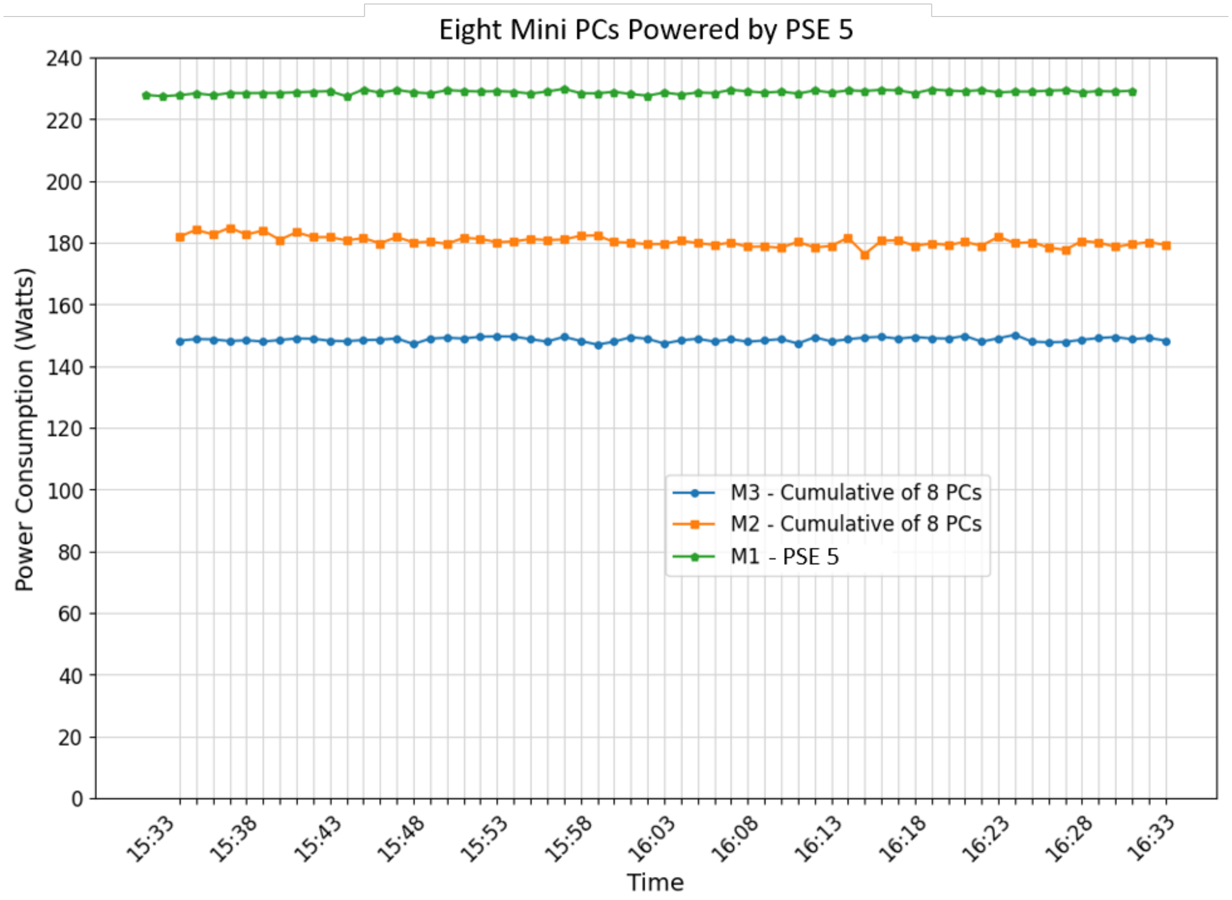

Figure 21 : Eight Mini PC on PSE 5

While this 18.5W power consumption is less than one third of the manufacturer rated max of 65W, the research team noted that the PoE Mini PC adapter tend to get very warm to the touch under these loading conditions. Analysis of the measured power data showed that approximately 6W of heat are dissipated by each PoE Mini PC adapter, resulting in a node efficiency of 82% (Table 21)

Table 20: Power Consumption of PoE Mini PC adapter on PSE 5

	PoE Mini PC Adapter					
	Measurement M3 (W)	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency[2] (%)	Switch Efficiency (%)	Node Efficiency (%)
PSE 5	148.65	180.22	228.87	65%	79%	82%

Similarly, the research team calculated the switch efficiency to be 79% and the total system efficiency of the PoE switch and PoE Mini PC adapter system to be 65%.

Next the research team connected 4 PoE Mini PC adapters to the four PSE 2 ports that support the IEEE 802.3 bt Type 3 power delivery standard. As with the previous test, a program was installed on the Mini PCs to load the CPU to 100%. When powered by the PSE 2, the four Mini PCs had an average power draw of 19.8W per computer, or 79.5W cumulatively (Figure 25).

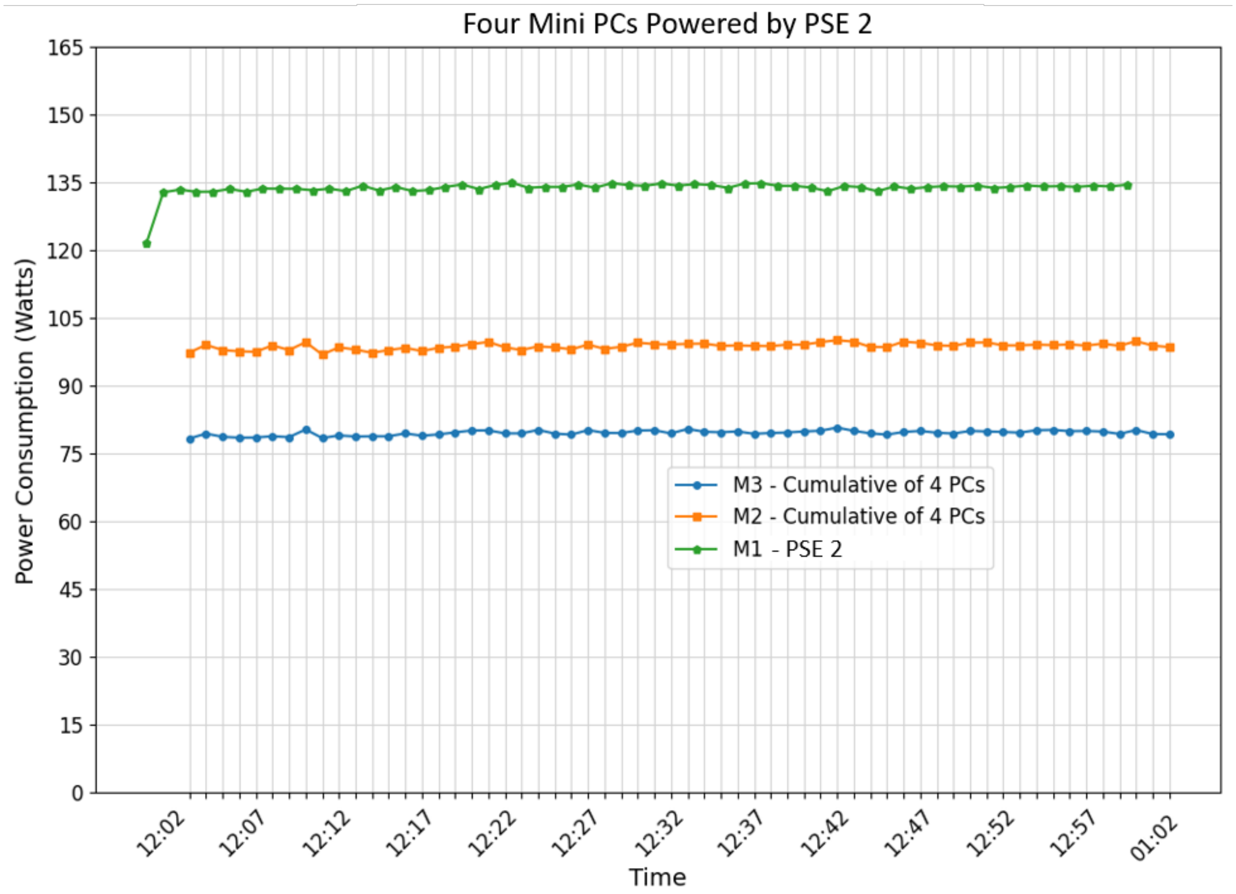

Figure 22: Four PoE Mini PC adapters on PSE 2

The efficiency of the PoE Mini PC adapter (node) under these conditions was calculated to be 81 percent, slightly lower than the 82 percent node efficiency observed in the previous test. Moreover, the total system efficiency was determined to be 59 percent (Table 22), lower than the 65 percent efficiency for the previous test, despite the PSE 2 being more fully loaded in relation to its total power capacity, than was the cast for the PSE 5 (55 percent of full load vs 35%).

Table 21: Power Consumption of PoE Mini PC adapter on PSE 2

PoE Mini PC Adapter

	Measurement M3 (W)	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency (%)	Switch Efficiency (%)	Node Efficiency (%)
PSE 2	79.51	98.72	133.67	59%	74%	81%

It is generally assumed that a higher relative percentage loading of a PoE switch will lead to greater efficiency for the same switch. While the PSE 5 switch, which was less fully loaded than the PSE 2 in this test, operated more efficiently, this does not necessarily contradict the assumption, considering the switches are from different manufacturers. The evidence from the system efficiency figures previously discussed indicates that the PSE 2 does indeed increase in efficiency with increasing load.

Finally, for comparison, the research team metered the manufacturer supplied AC/DC power supply for the Mini PC per Configuration 3 for a one-hour test (Figure 26). This AC/DC wall adapter accepts 120-240VAC and can output 19V DC at 3.4A for a total power max power output of 65W. Similarly to the previous two tests, the Mini PC CPU was programmatically loaded to 100 percent to ensure maximum power draw from the computer.

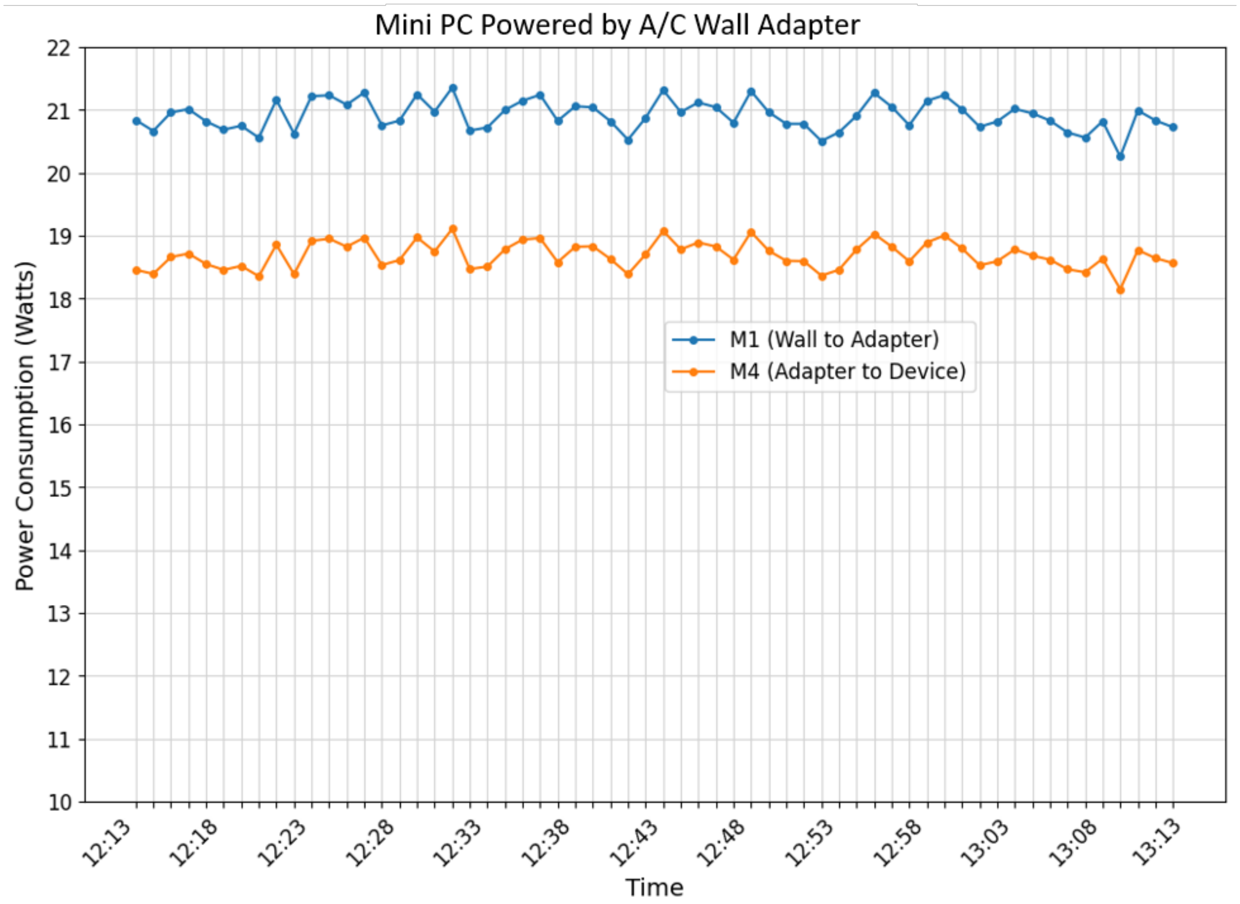

Figure 23: Mini PC powered by AC wall adapter

The research team found that, when powered from the manufacturer supplied AC/DC wall adapter, the Mini PC consumes about 18.7W (Table 23) which is comparable to the 18.5W consumed when powered by the PSE 5.

Table 22: Power Consumption of Mini PC on Wall Adapter

	Mini PC		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
AC/DC Power	18.7	20.9	89%

Overall, the AC power adapter consumed 20.9W and delivered 18.7W to the Mini PC, achieving a power supply efficiency of 89 percent. This efficiency surpasses the overall system efficiencies observed with both the PSE 5 and PSE 2 switches. Consistent with observations for other devices, using the power adapter proved more efficient than utilizing PoE switches to power the Mini PC.

POE LED DRIVER

For this report, the research team exclusively used the PSE 5 switch in the evaluation of PoE LED driver. The team used two 45W LED luminaires per PoE LED driver, cumulatively reaching the maximum capacity of 90W per port allowed by the PSE 5 switch. To achieve this setup, the team used the Manufacturer 3 controller to programmatically configure each PoE LED driver to have a maximum wattage of 45W, configured the PoE LED driver to operate in constant current mode, and then leveraged its built-in features to automatically detect and apply the suitable drive current. As with all previous tests, the research team allowed the luminaires and PoE LED drivers to stabilize before conducting a one-hour data collection period with one-minute sampling intervals.

In this configuration, the PSE 5 switch, with eight connected PoE LED drivers loaded with 90W of LED luminaires operating at full brightness, drew a total of 799.2W from the A/C source (Figure 27).

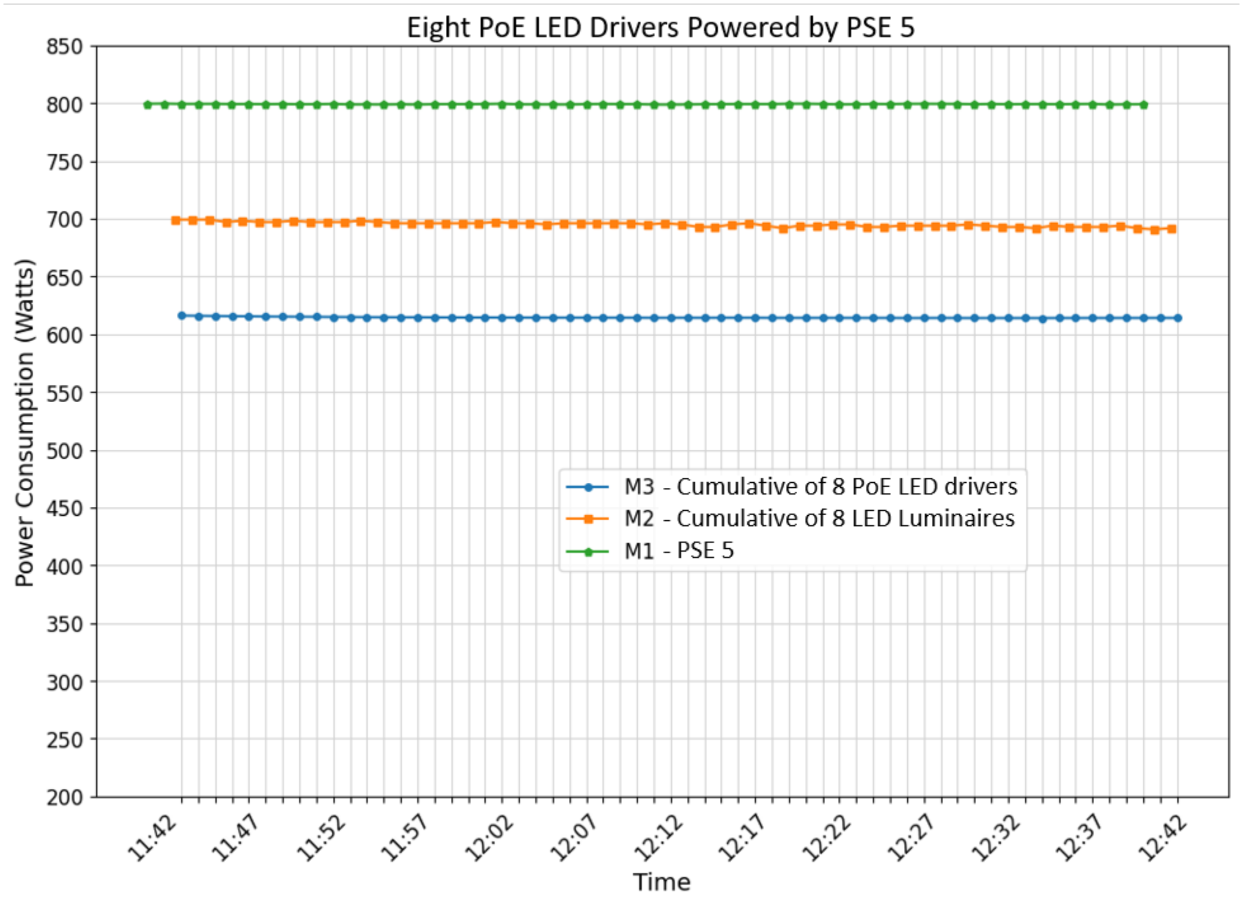

Figure 24: Eight LED Luminaires on PSE 5

The PSE 5 delivered a total of 695.2W to the PoE LED drivers (86.9W each) which subsequently provided a total of 636.86W to light fixtures. While the system is programmed to provide 45W to each light fixture, each light fixture actually received around 40W (with two luminaires per PoE LED driver). The total system efficiency for the fully loaded PSE 5 switch was calculated to be 80 percent (Table 24).

Table 23: Power Consumption of LED Luminaires on PSE 5

	LED Luminaires					
	Measurement M3 (W)	Measurement M2 (W)	Measurement M1 (W)	Total System Efficiency2 (%)	Switch Efficiency (%)	Node Efficiency (%)
PSE 5	636.86	695.21	799.21	80%	87%	92%

Next, the research team powered two of the same 45W luminaires, each with a dedicated 45W constant current LED. The LED driver was selected to match the voltage and current output of the PoE LED driver for the same LED fixture. These LED drivers were metered per Configuration 3 for a one-hour period (Figure 28).

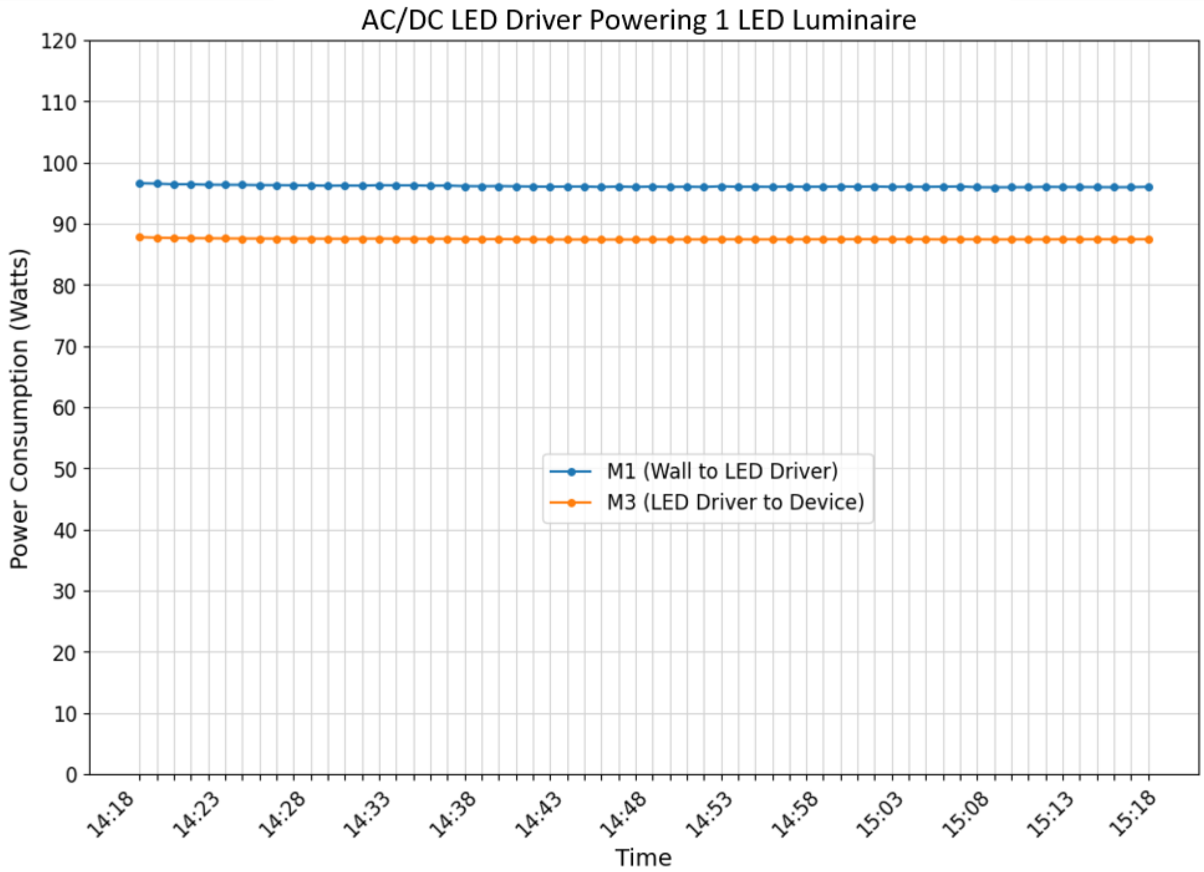

Figure 25: LED Troffer on AC/DC LED Driver

The AC/DC LED driver was able to deliver 43.7W to each LED luminaire and had a total system efficiency of 91 percent (Table 25).

Table 24: Power Consumption of AC/DC LED driver for the LED Luminaire

	LED Troffer		
	Measurement M4 (W)	Measurement M1 (W)	Power Supply Efficiency (%)
Meanwell Driver	87.47	96.11	91%

PoE Switch Efficiencies

To quantify the electrical efficiency of each PoE switch, the research team subjected each switch to a series of tests under varying load conditions. By incrementally increasing the number and type of connected devices, the team measured the efficiency across the switch's total load range, from low to high utilization. This approach provided a comprehensive understanding as to how each switch performed under different operational loads, highlighting trends in energy efficiency and identifying optimal load conditions for maximizing performance.

PSE 1

The PSE 1, the smallest switch tested in terms of output capacity, was evaluated with loads ranging from 14W to 100.8W (Table 26). It was subjected to incrementally larger loads, with each test conducted over a period of one hour, to assess its performance and efficiency under varying conditions.

Table 25: Loading Schemes for PSE 1

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 1	4 x PoE Cameras	120W	14.22	29.06	12%	49%
Load 2	2 x PoE PAC + 2 x PoE Access Points		33.45	49.11	28%	68%
Load 3	3 x Luminaires Each Operating at 30W		76.67	113.81	64%	67%
Load 4	4 x Motorized Shades + 4 x VaV Controllers		80.12	100.85	67%	79%
Load 5	4 x Luminaires Each Operating at 30W		145.22	145.22	84%	69%

- **Load 1**: The switch was loaded with four PoE cameras, each drawing an average of 3.5W, resulting in a 12 percent load and an efficiency of 49 percent.
- **Load 2**: When the load increased to 28 percent, with two PoE access controllers and two PoE access points, the efficiency increased to 68 percent. This represents a 133 percent increase in load from Load 1, resulting in a 38.8 percent increase in efficiency.
- **Load 3**: Three luminaires, each operating at 30W (the maximum output per port on the PSE 1), were powered by the switch. This scenario represented 64 percent of the switch's capacity. Despite this significant increase in load (from 28 percent to 64 percent), the efficiency slightly decreased to 67 percent, marking a one percent decrease from the previous load.
- **Load 4**: This test involved powering four motorized shades and four VAV controllers, cumulatively drawing an average of 80.12W, representing 67 percent of the switch's total

capacity. Despite the slight increase in load from Load 3 (64 percent to 67 percent), the efficiency increased to 79 percent, reflecting an 18% percent improvement.

- **Load 5**: The final test involved four luminaires, each operating at 30W, bringing the load to 84 percent of the switch's capacity. This represents a 25.37 percent increase in load from Load 4. However, the efficiency dropped to 69 percent, reflecting a 10 percent decrease compared to the previous load scenario.

While efficiency does increase with load percentage, the data suggests that the switch is designed to operate most efficiently within its mid-load range rather than at full capacity. This indicates that the switch may be optimized for maximum efficiency at moderate loads, with diminishing returns as it approaches its maximum capacity.

The analysis of the of switch efficiency versus load percentage for the PSE 1 shows a clear trend where efficiency increases with load percentage up to a certain point, after which it begins to fluctuate (Figure 29).

Figure 26: PSE 1 - loading vs. efficiency.

- **Initial Increase (Load 1 to Load 2)**: At lower load percentages (around 12 percent to 2 percent), the switch efficiency improves significantly, climbing from 49 percent at Load 1 to 68 percent at Load 2. This suggests that the switch becomes more efficient as it begins to handle more substantial loads, moving out of its lower operational range.
- **Stability (Load 2 to Load 3)**: Between Load 2 and Load 3, the efficiency remains relatively stable at around 67 percent despite the load increasing from 28 percent to 64 percent. This

plateau indicates that the switch may have reached an optimal range for efficiency at this mid-level load.

- **Efficiency Peak (Load 4)**: At Load 4, with a 67 percent load, efficiency peaks at 79 percent. This suggests that the switch is optimized for this moderate to high load range, where it operates most efficiently.
- **Decline (Load 4 to Load 5)**: After Load 4, the efficiency drops slightly to 69 percent at an 84 percent load (Load 5). This decline indicates that as the switch approaches its maximum capacity, efficiency begins to decrease, highlighting the potential limitations of the switch's design when operating near full capacity.

Overall, the data suggests that the PSE 1 is most efficient when operating within a mid-load range, around 60 to 70 percent of its capacity. Efficiency gains are evident as the load increases from low to moderate levels, but these gains diminish and even reverse as the switch nears its full capacity.

PSE 2

The research team evaluated the PSE 2 switch under various loading configurations to assess its efficiency at different capacities (Table 27). Unlike the PSE 1, which has a total switch capacity of 120W, the PSE 2 offers increased power output, allowing 60W per port for four ports simultaneously with a maximum PoE output of 240W, though this must be programmatically configured through the command line interface (CLI).

Table 26: Loading Schemes for PSE 2

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 1	4 x PoE Cameras + 1 * PoE Access Controller	240	22.09	52	11%	49%
Load 2	4 x PoE Access Controllers + 4 x PoE Access Points		63.24	101.19	26%	62%
Load 3	2 x PoE Mini PCs + 2 x Luminaires @ 30W		91.02	145.93	38%	62%
Load 4	2 x Motorized Shades + 4 x VaV Controllers +2 x Luminaires (60W & 30W)		151.71	194.05	63%	78%
Load 5	4 x USB-C		218.37	262.31	91%	83%

- **Load 1**: This setup consisted of powering four PoE cameras and one PoE access controller, resulting in a switch load of 11 percent and an efficiency of 49 percent.
- **Load 2**: When the load increased to 26 percent, by powering four PoE access controllers and four PoE access points, the efficiency improved to 62 percent. This represents a 136 percent increase in load, leading to a 26.5 percent improvement in efficiency.
- **Load 3**: This next configuration involved powering two PoE Mini PCs adapters and two luminaires, each operating at 30W. The total load reached 38 percent, with the efficiency remaining at 62 percent. Despite a 46.2 percent increase in load, there was no change in efficiency.
- **Load 4**: This setup included powering two motorized shades, four VAV controllers, and two luminaires (one drawing 60W and the other 30W), raising the load to 63 percent. This 65.8 percent increase in load significantly boosted efficiency to 78 percent, marking a 25.8 percent improvement.
- **Load 5**: The final loading scheme consisted of four USB-C devices, resulting in a switch load of 91 percent and an efficiency of 83 percent. This represents a 44.4 percent increase in load from Load 4, with a 6.4 percent improvement in efficiency.

The data indicates a clear trend: as the switch load increases, efficiency improves substantially, particularly at mid-range loads. However, efficiency gains diminish at higher load percentages.

The analysis of switch efficiency versus load percentage for the PSE 2 demonstrates a consistent improvement in efficiency as the load increases, with some notable characteristics at different load levels (Figure 30).

Figure 27: PSE 2 - loading vs efficiency

- **Initial Increase (Load 1 to Load 2):** The switch starts with a low efficiency of 49 percent at an 11 percent load (Load 1), but as the load increases to 26 percent in Load 2, the efficiency significantly improves to 62 percent. This initial jump indicates that the switch quickly becomes more efficient as it begins to handle more substantial loads, suggesting it operates sub-optimally at very low loads.

- **Plateau (Load 2 to Load 3):** Between Load 2 (26 percent) and Load 3 (38 percent), efficiency remains steady at 62 percent. This plateau suggests that while the switch can maintain a moderate level of efficiency at mid-range loads.

- **Substantial Gain (Load 3 to Load 4):** The most significant gain in efficiency occurs between Load 3 (38 percent) and Load 4 (63 percent), where efficiency jumps from 62 percent to 78 percent. This sharp increase indicates that the switch is likely designed to perform optimally at moderate to higher loads, where it can maximize its power delivery efficiency.

- **Moderate Improvement (Load 4 to Load 5):** Finally, from Load 4 (63 percent) to Load 5 (91 percent), the efficiency continues to improve, though at a slower rate, reaching 83 percent. This suggests that while the switch remains efficient as it approaches full capacity, the gains in efficiency begin to taper off, implying that the switch is near its optimal operating point.

Overall, the PSE 2 shows a clear trend of increasing efficiency with higher loads, particularly excelling as it transitions from mid-range to higher loads. Compared with the PSE 1, which showed efficiency peaking at mid-loads and then declining as it approached full capacity, the PSE 2 demonstrates more sustained efficiency gains across a wider range of loads. This suggests that the PSE 2 is better optimized for higher performance across a broader spectrum of load conditions, making it more suitable for environments where higher capacity and consistent efficiency are required.

PSE 4

The PSE 4 switch's efficiency was evaluated under a range load conditions, resulting a range of efficiency responses to increasing PoE wattages. The same five load configurations tested on the PSE 2 were used for the PSE 4 switch. Although both switches have an identical maximum capacity of 240W, the PSE 4 switch restricts ports 1 to 4 to a maximum of 60W per port and ports 5 to 8 to a maximum of 30W per port.

Table 27: Loading Schemes for the PSE 4

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 1	4 x PoE Cameras + 1 * PoE Access Controller	240	22.84	40	10%	57%
Load 2	4 x PoE Access Controllers + 4 x PoE Access Points		60.82	84.26	25%	72%
Load 3	2 x PoE Mini PCs adapters + 2 x Luminaires @ 30W		90.86	129	38%	70%
Load 4	2 x Motorized Shades + 4 x VaV Controllers +2 x Luminaires (60W & 30W)		150.63	172.04	63%	88%
Load 5	4 x USB-C		217.97	249.51	91%	87%

- **Load 1**: This setup included four PoE cameras and one PoE access controller. The switch operated at 10 percent load, drawing 26.5W and achieving an efficiency of 66 percent.
- **Load 2**: The load increased to 60.8W, representing 25 percent of the switch's capacity, and consisted of four PoE access controllers and four PoE access points. The efficiency increased to 72 percent.
- **Load 3**: This configuration consisted of powering two PoE Mini PCs and two luminaires, each operating at 30W. The two Mini PCs were connected to ports 1 and 3, as these ports can provide 60W. The switch load reached 38 percent, with a PoE wattage of 90.8W and an efficiency of 70 percent. This loading scheme resulted in a two percent decrease in efficiency as the load increased by 13 percent.

- **Load 4**: This loading scheme included two motorized shades, four VAV controllers, and two luminaires (one drawing 60W and the other 30W). The 60W luminaire was placed on one of the higher-capacity ports (1 to 4). This configuration resulted in a 63 percent load on the switch, with a PoE wattage of 150.63W, achieving the highest efficiency of 88 percent.
- **Load 5**: The final loading scheme consisted of four USB-C devices, resulting in a switch load of 91 percent, a PoE wattage of 217.97W, and an efficiency of 87 percent. Beyond a 60 percent load, the increase in switch load did not result in significant gains in efficiency.

The analysis of switch efficiency versus load percentage for the PSE 4 switch demonstrates a generally linear proportional trend between efficiency and load percentage, with several key characteristics at different load levels (Figure 31).

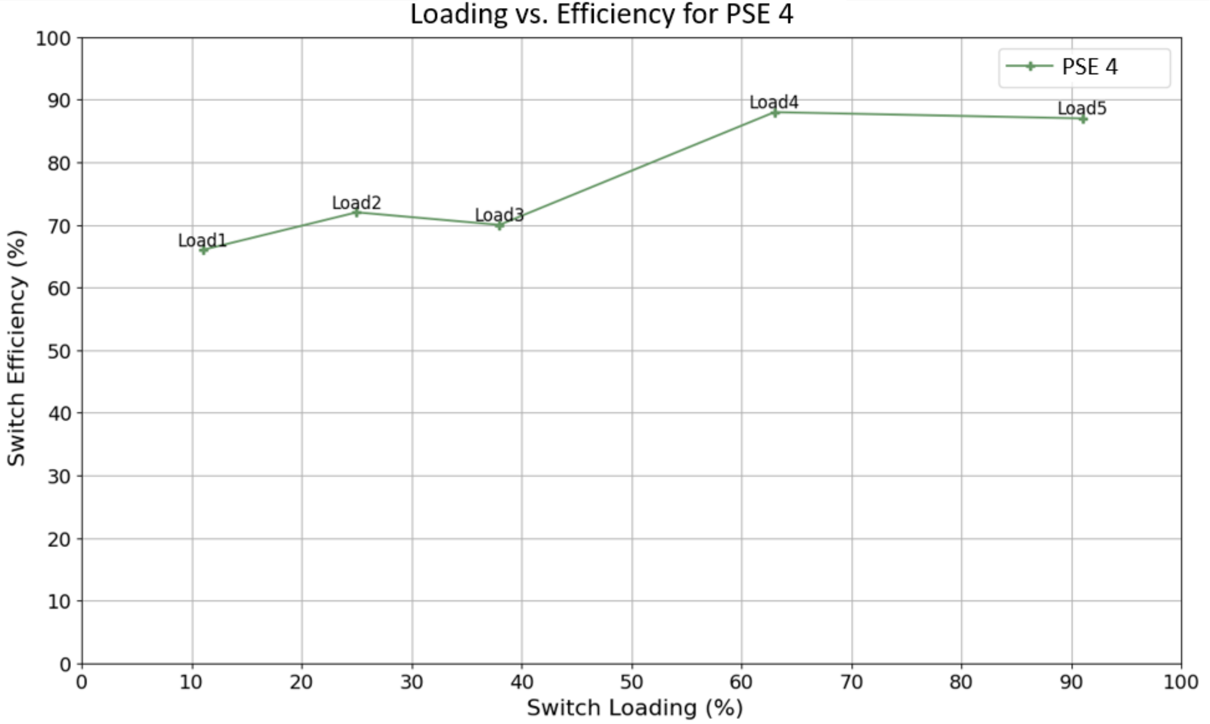

Figure 28: PSE 4 - loading vs. efficiency

- **Initial increase (Load 1 to Load 2)**: The switch starts with a relatively high efficiency of 66 percent at a 10 percent load (Load 1). As the load increases to 25 percent in Load 2, efficiency improves to 72 percent. This initial increase indicates that the switch is efficient at lower loads compared to other similarly sized switches.
- **Minor Fluctuation (Load 2 to Load 3)**: Between Load 2 (25 percent) and Load 3 (38 percent efficiency slightly decreases from 72 percent to 70 percent, even as the load increases. This small drop suggests that the switch may encounter some inefficiencies as it transitions through this mid-range load, indicating that it does not maintain a perfectly linear improvement in efficiency as load increases.

- **Significant Gain (Load 3 to Load 4):** The most substantial gain in efficiency occurs between Load 3 (38 percent) and Load 4 (63 percent), where efficiency jumps from 70 percent to 88 percent. This sharp increase highlights that the switch is designed to perform optimally at moderate to higher loads, where it can maximize its power delivery efficiency.
- **Efficiency Plateau (Load 4 to Load 5):** From Load 4 (63 percent) to Load 5 (91 percent), efficiency slightly decreases from 88 percent to 87 percent. This indicates that as the switch approaches its maximum capacity, efficiency gains taper off, and the switch stabilizes in its performance, suggesting that it is near its optimal operating point at these higher loads.

Overall, the PSE 4 8-port switch shows a generally increasing trend in efficiency with higher loads, with the most significant gains occurring between moderate and high load percentages. Notably, compared to the PSE 1 and PSE 2, the PSE 4 switch displays higher efficiency even at lower load levels. This suggests that the PSE 4 switch is not only optimized for moderate to high loads but also performs efficiently at lower loads, achieving peak efficiency slightly earlier and maintaining solid performance across a broader range of load conditions.

PSE 5

The PSE 5 switch was evaluated after the PSE 4 switch, offering a higher capacity with the ability to provide up to 720W of total PoE power. Because of its increased capacity, this switch was tested with larger load combinations compared to the previous devices (Table 29).

Table 28: Loading Schemes for the PSE 5

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 1	4 x PoE Cameras + 4 * PoE Access Controller	720	62.14	89.46	9%	69%
Load 2	3 x Motorized Shades + 3 x PoE Access Points + 2 Luminaires		184.4	242.35	26%	76%
Load 3	4 x USB-C + 2 x PoE Mini PCs		276.93	395.12	38%	70%
Load 4	4 x VaV Controllers +6 x Luminaires (90W)		494.6	650	69%	76%
Load 5	8 x Luminaires (90W)		619.56	813	86%	76%

- **Load 1**: The switch powered four PoE cameras and four PoE access controllers. This setup consumed 62.14W, representing nine percent of the switch's capacity. The power drawn from the wall was 89.46W, resulting in an efficiency of 69%.
- **Load 2**: This setup involved three motorized shades, three PoE access points, and two luminaires. The load consumed 184.4W, which was 26% of the switch's total capacity. The corresponding wall power draw was 242.35W, yielding an efficiency of 76 percent.
- **Load 3**: The switch powered four USB-C devices and two PoE Mini PCs, consuming a total of 276.93W, or 38 percent of the switch's capacity. The wall power draw increased to 395.12W, but the efficiency decreased to 70 percent. This drop in efficiency, despite the higher load, indicates a non-linear relationship between load and PSU performance.
- **Load 4**: The switch powered four VAV controllers and six luminaires, resulting in a load of 494.6W, or 69 percent of the switch's capacity. The wall power draw was 650W, maintaining an efficiency of 76 percent. At this higher loading percentage, the efficiency stabilized, likely reflecting the PSU operating closer to its optimal efficiency range, where the overhead is minimized and the power delivery becomes more consistent.
- **Load 5**: The switch was tested with eight luminaires, each drawing 90W, leading to a total consumption of 619.56W, or 86 percent of the switch's capacity. The wall power draw further increased to 813W, but the efficiency remained consistent at 76 percent, similar to the previous configuration. This stability in efficiency at higher loads suggests that the PSU's efficiency curve plateaus when operating at a substantial portion of its capacity, indicating that additional load does not significantly impact efficiency.

The analysis of switch efficiency versus load percentage for the PSE 5 switch reveals a mixed trend in efficiency as the load increases, with several notable observations at different load levels (Figure 32).

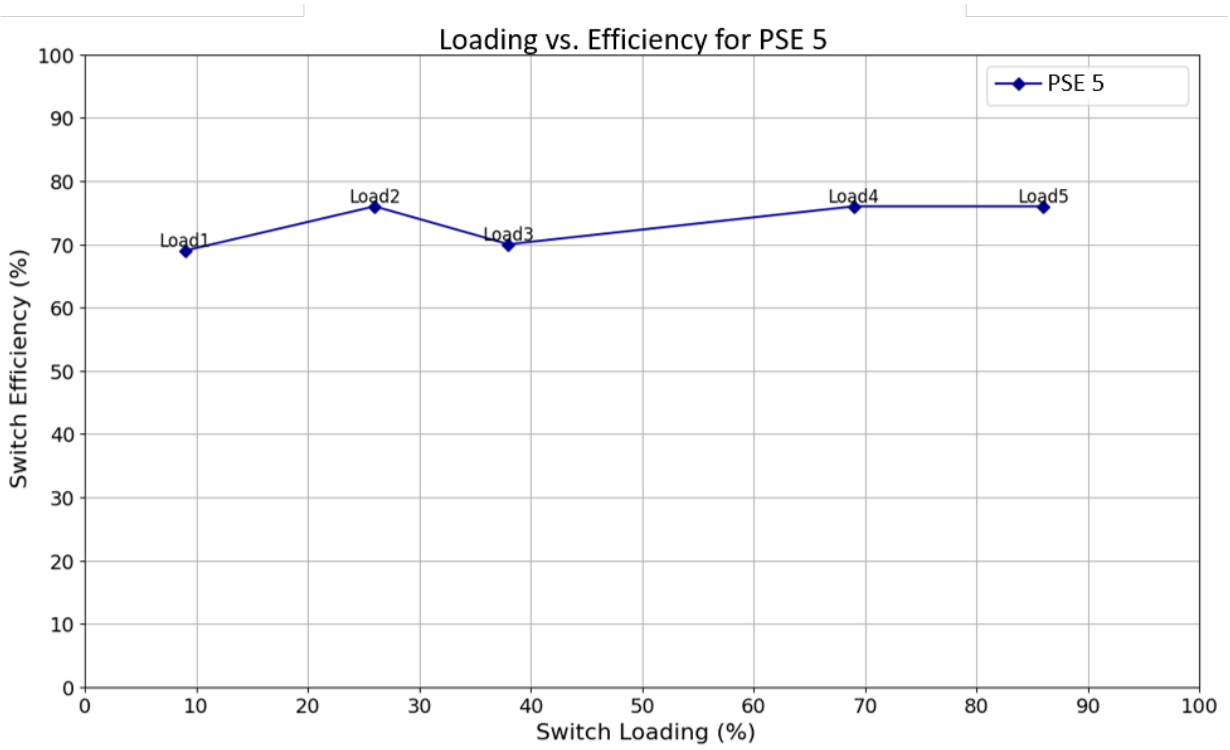

Figure 29: PSE 5 - loading vs efficiency

- **Initial Performance (Load 1 to Load 2)**: The switch starts with an efficiency of 69 percent at a nine percent load (Load 1). As the load increases to 26 percent in Load 2, the efficiency improves to 76 percent. This initial increase indicates that the switch becomes more efficient as it begins to handle larger loads, suggesting that it is capable of achieving higher efficiency with moderate loading.
- **Efficiency Drop (Load 2 to Load 3)**: Between Load 2 (26 percent) and Load 3 (38 percent), efficiency decreases from 76 percent to 70 percent, even though the load increases. This drop in efficiency, despite the higher load, suggests a non-linear relationship between load and power supply unit (PSU) performance, potentially due to inefficiencies arising at this particular mid-range load.
- **Stabilization at Higher Loads (Load 3 to Load 5)**: From Load 3 (38 percent) through Load 4 (69 percent) to Load 5 (86 percent), efficiency stabilizes around 76 percent. This indicates that the switch operates with consistent efficiency as it approaches higher load percentages, likely reflecting the PSU operating closer to its optimal efficiency range. The lack of further significant efficiency gains at higher loads suggests that the switch has reached a plateau, where additional load does not significantly enhance or reduce efficiency.

Overall, the PSE 5 switch demonstrates that while efficiency is slightly proportional to load, it remains more or less constant across the entire loading range. Starting with 69 percent efficiency at just nine percent load and reaching 76 percent at the highest load (86 percent), the switch maintains a fairly consistent efficiency level regardless of the load percentage. This suggests that the PSE 5 switch is designed to perform efficiently across a wide range of loads, with only minor variations in efficiency as the load increases, making it a stable option for handling both low and high load conditions.

PSE 3

The performance of the high-capacity PSE 3 switch, with a total PoE power output of 2160W, was evaluated under various load conditions (Table 30). Due to its large capacity, each test scenario included two or more luminaires, as these can be programmed to draw up to 90W each.

Table 29: Loads Used For PSE 3 24 Port

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 1	4 x PoE Cameras + 4 * PoE Access Controller + 2 x Luminaires	2160	211.82	352.21	10%	60%
Load 2	2 x Motorized Shades + 4 x Luminaires + 3 x USB-C		498.07	763.98	23%	65%
Load 3	4 x PoE Access Points + 4 x PoE Mini PCs + 8 x Luminaires		718.46	912.65	33%	79%
Load 4	12 x Luminaires + 8 x USB-C + 2 x PoE Access Controller + 2 VaV		1409.17	1726.7	65%	82%
Load 5	16 x Luminaires (90W) + 8 x USB-C		1668.555	2057.88	77%	81%
Load 6	21 x Luminaires (90W) + 3 x USB-C		1808.01	2131	84%	85%

- **Load 1**: The switch powered four PoE cameras, four PoE access controllers, and two luminaires. The PoE output was 211.82W, with a total switch consumption of 352.21W. This represented a ten percent load on the switch, resulting in an efficiency of 60 percent
- **Load 2**: The setup included two motorized shades, four luminaires, and three USB-C devices. The PoE wattage increased to 498.07W, while the switch consumed 763.98W, corresponding to a 23 percent load and an efficiency of 65 percent.

- **Load 3**: This test involved four PoE access points, four PoE Mini PCs, and eight luminaires. The PoE wattage was 718.46W, and the total switch consumption was 912.65W, equating to a 33 percent load and a 79 percent efficiency.
- **Load 4**: The switch powered twelve luminaires, eight USB-C devices, two PoE access controllers, and two VAV controllers. The PoE wattage was 1409.17W, with a total consumption of 1726.7W. This setup resulted in a 65 percent load on the switch, with an efficiency of 82 percent.
- **Load 5**: Sixteen luminaires and eight USB-C devices were connected, leading to a PoE wattage of 1668.55W and a total consumption of 2057.88W. This represented a 77 percent load on the switch, with an efficiency of 81 percent.
- **Load 6**: The final test involved twenty-one luminaires and three USB-C devices. The PoE wattage reached 1808.01W, and the total consumption was 2131W, resulting in an 84 percent switch load and an efficiency of 85 percent.

The analysis of switch efficiency versus load percentage for the high-capacity PSE 3 switch reveals a clear trend of improving efficiency as the load increases, with several distinctive patterns emerging at different load levels (Figure 33).

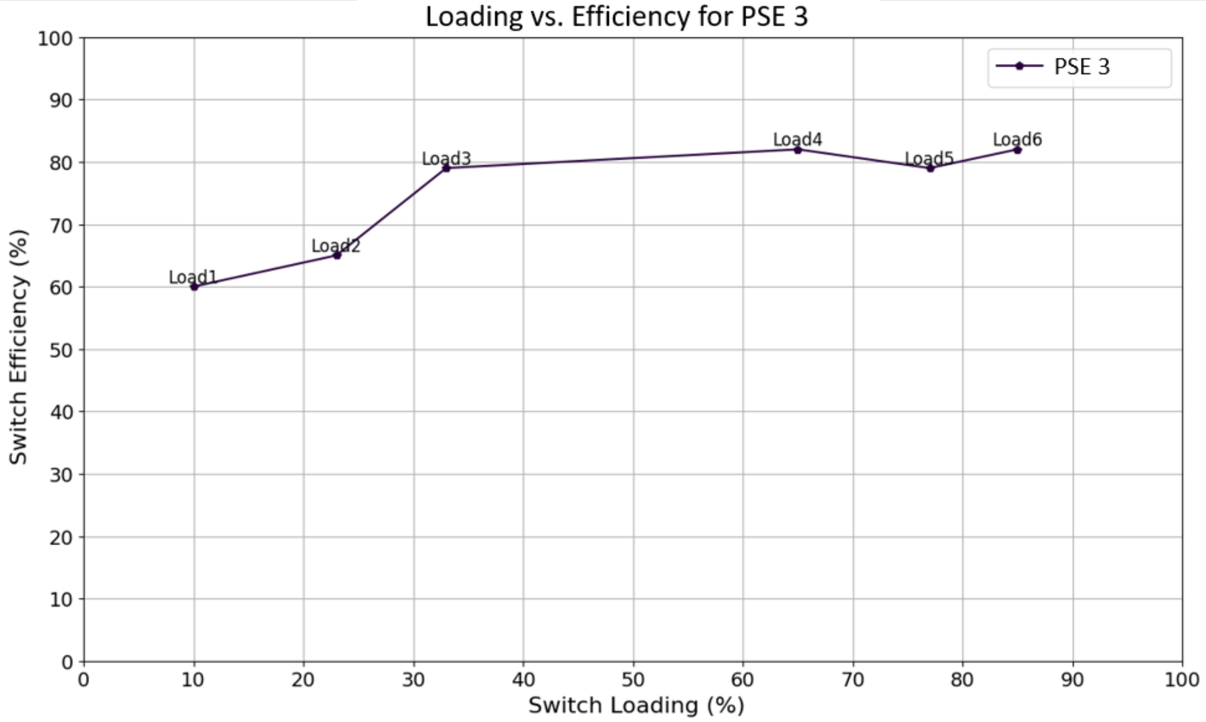

Figure 30: PSE 3 24 Port - Loading vs Efficiency

- **Gradual Improvement (Load 1 to Load 2)**: Starting with a ten percent load, the switch achieves an efficiency of 60 percent. As the load increases to 23 percent in Load 2, efficiency improves modestly to 65 percent. This gradual improvement suggests that the switch's efficiency at very low loads is suboptimal, but it begins to stabilize and improve as more devices are connected, likely due to better utilization of its internal power distribution.

- **Significant Efficiency Jump (Load 2 to Load 3)**: Between Load 2 (23 percent) and Load 3 (33 percent), there is a significant efficiency gain, jumping from 65 percent to 79 percent. This sharp increase indicates that the PSE 3 operates most efficiently when transitioning from lower to mid-range loads, where it can leverage its higher capacity to deliver power more effectively.
- **Efficiency Plateau (Load 3 to Load 5)**: From Load 3 (33 percent) to Load 4 (65 percent) and into Load 5 (77 percent), the efficiency stabilizes around the low 80s, peaking at 82 percent and slightly dipping to 81 percent. This plateau suggests that while the switch maintains high efficiency across this mid-to-high load range, it may not be significantly optimized beyond this point, with only marginal improvements as the load increases.
- **Final Efficiency Gain (Load 5 to Load 6)**: As the switch load increases further to 8 percent in Load 6, the efficiency rises again, reaching 85 percent. This final increase implies that the PSE 3 has a design that slightly favors higher loads, achieving peak efficiency just before reaching full capacity.

Overall, the PSE 3 shows a strong performance in terms of efficiency when transitioning from mid to high loads. The switch's ability to maintain and slightly improve efficiency at higher loads suggests it is well-suited for environments that require consistent and reliable power delivery across a range of larger connected devices.

PSE 6

The PSE 6 switch, with a capacity of 2160W, was tested under various load configurations (Table 31) to assess its operational efficiency. This switch has a capacity similar to the 24-port PSE 3 discussed earlier, and the same loading profiles were used for comparison.

Table 30: Loading schemes for the PSE 6

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 1	4 x PoE Cameras + 4 * PoE Access Controller + 2 x Luminaires	2160	213.46	313.56	10%	68%
Load 2	2 x Motorized Shades + 4 x Luminaires + 3 x USB-C		535.18	685.62	25%	78%

		Switch Capacity (W)	PoE Wattage [M2 or M3] (W)	M1 (W)	Switch Load %	Switch Efficiency %
Load 3	4 x PoE Access Points + 4 x PoE Mini PCs + 8 x Luminaires		717.74	930	33%	77%
Load 4	12 x Luminaires + 8 x USB-C + 2 x PoE Access Controller + 2 VaV		1482.82	1803.59	69%	82%
Load 5	16 x Luminaires (90W) + 8 x USB-C		1742.75	2133	81%	82%
Load 6	22 x Luminaires (90W) + 2 x USB-C		2233.39	1827.60	85%	82%

- **Load 1:** The setup included four PoE cameras, four PoE access controllers, and two luminaires, resulting in a total PoE load of 213.46W and a total AC load of 313.56W. This represented a ten percent load on the switch, with an overall efficiency of 68 percent.
- **Load 2:** The switch powered two motorized shades, four luminaires, and three USB-C devices, consuming 535.18W of power. The total power draw from the wall was 685.62W, indicating a 25 percent load on the switch and an efficiency of 78 percent.
- **Load 3:** This configuration involved four PoE access points, four PoE Mini PCs, and eight luminaires at full brightness, each consuming 90W. The total power consumption was 717.74W, with a wall power draw of 930W, equating to a 33 percent load on the switch and a 77 percent efficiency. The efficiency decreased by one percent from Load 2 to Load 3.
- **Load 4:** The switch was connected to twelve luminaires, eight USB-C devices, two PoE access controllers, and two VAV controllers. The load consumption was 1482.82W, with a power draw of 1803.59W from the wall. This configuration represented a 69 percent load on the switch, with an efficiency increase of five percent, compared with Load 3 at 82 percent.
- **Load 5:** Sixteen luminaires, each operating at 90W, and eight USB-C devices were connected, resulting in a total PoE load of 1742.75W and a wall draw of 2133W. This scenario equated to an 81 percent load on the switch, with an efficiency of 82 percent.
- **Load 6**: The final test involved twenty-two luminaires, each operating at 90W, and two USB-C devices. The total PoE load reached 2233.39W, with a wall power draw of 1827.60W. This represented an 85 percent load on the switch, maintaining an efficiency of 82 percent.

The analysis of switch efficiency versus load percentage for the PSE 6 switch shows a generally stable and consistent performance across various load conditions, with a few key observations (Figure 34).

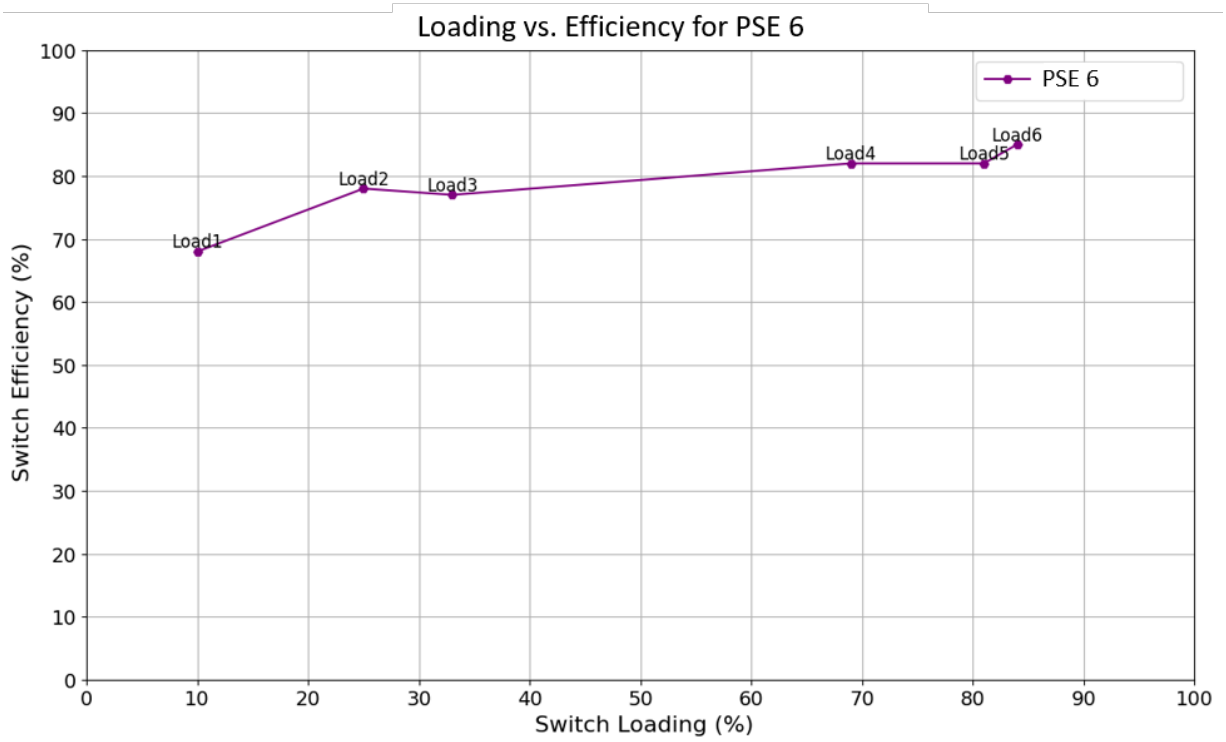

Figure 31: PSE 6 - Loading vs Efficiency

- **Initial Performance (Load 1 to Load 2)**: The switch starts with an efficiency of 68 percent at a ten percent load (Load 1). As the load increases to 25 percent in Load 2, efficiency improves significantly to 78 percent. This sharp initial improvement suggests that the switch quickly becomes more efficient as it transitions from low to moderate loads, likely due to better power distribution and utilization at these load levels.
- **Hypothesis on Mid-Range Efficiency Dip (Load 2 to Load 3)**: Between Load 2 (25 percent) and Load 3 (33 percent), there is a slight decrease in efficiency from 78 percent to 77 percent. One possible explanation for this mid-range dip is that the switch is equipped with two discrete power supplies. In this scenario, one power supply may become fully loaded and operate efficiently, while the second power supply begins to take on the additional load but is not yet fully utilized, leading to a temporary reduction in overall efficiency. This hypothesis assumes that the power supplies work sequentially—where one is fully loaded before the other begins to provide power—rather than both power supplies always sharing the load equally.
- **Stabilization and Consistency at Higher Loads (Load 4 to Load 6)**: As the load increases from 33 percent in Load 3 to 69 percent in Load 4, efficiency rebounds to 82 percent. The efficiency remains stable around this level as the load increases further to 85 percent in Load 6. This consistent performance at higher loads suggests that once both power supplies

are more fully utilized, the switch operates at optimal efficiency. The design likely ensures steady efficiency at higher load levels, where both power supplies can share the load more effectively and operate closer to their peak efficiency.

Overall, the PSE 6 switch exhibits a stable efficiency profile with significant gains as the load increases from low to moderate levels. The slight dip in mid-range efficiency might be attributed to the activation of the second power supply, assuming that the power supplies are loaded sequentially rather than simultaneously. As the load continues to increase, the switch stabilizes and maintains consistent efficiency, making it well-suited for high-capacity operations. Compared with the PSE 3, which also showed a notable efficiency gain at higher loads, the PSE 6 switch demonstrates similar behavior in stabilizing at higher loads, indicating both switches are optimized for reliable performance in demanding, high-capacity environments.

Centralized vs. Decentralized System Efficiency

One of the main goals of this research project was to design and evaluate scaled PoE Microgrids at the whole-building or floor level, using commercially available PoE-enabled switches. Two primary configurations were considered: one that utilizes separate, appropriately sized PoE switches for each building system (decentralized), and another that employs a single, larger PoE switch to aggregate all building systems (centralized). The centralized configuration involves two large switches, the PSE 3 and the PSE 6, both of which were configured to function as the central hubs. Each switch was equipped identically, with eight ports dedicated to eight 90W luminaires, eight ports powering eight PoE Mini PCs, and the remaining eight ports filled with four PoE PAC and four PoE cameras. This setup was designed to represent a typical commercial floor space, where multiple electronic devices are powered by a single PoE switch.

PSE 3 CENTRALIZED

In the centralized configuration, the largest load for the PSE 3 switch was the eight luminaires, each programmed via Manufacturer 3 controller to draw 90W. The M3 measurement, which captures the power drawn after the PoE node and includes both line losses and losses due to the PoE LED driver, recorded a total of 625.84W for the eight luminaires.

The second largest load for this switch was the cumulative power draw of the eight PoE Mini PCs. Each of the eight mini-PCs were configured to run at full power draw, using a Python application that fully utilized all available CPU cores and maximized RAM usage throughout the testing period. Each Mini PC drew an average of 18.865W, resulting in a cumulative total of 150.92W for all eight PCs.

The next largest load for the centralized architecture was comprised of the PoE PAC and PoE cameras, which had relatively smaller PoE power draws compared to the Mini PCs. The four PoE PACs drew a collective 46.92W, while the four PoE cameras accounted for a total of 13.28W. These measurements were M2 measurements, as there were no intermediary drivers or power splitters involved, unlike with the luminaires and Mini PCs. With all connected devices powered and metered for an hour, the combined PoE load on the PSE 3 switch totaled 836.99W (Table 32).

Table 31: Centralized Loading - PSE 3

PSE 3 24Port - Centralized	Quantity	Wattage (W)
Luminaires	8	625.84

PoE Mini PCs	8	150.92
PoE PAC	4	46.92
PoE Cameras	4	13.28
PoE Wattage	**24**	**836.96**
PSE 3 24 Port Power Supply 1	1	511.81
PSE 3 24 Port Power Supply 2	1	549.36
Total Consumed by the Switch		**1061.17**
System Efficiency		79%

To supply this PoE output power along with the switch's internal power consumption, the PSE 3 is equipped with two discrete internal power dedicated supplies. The research team metered both power supplies throughout the duration of this test. Power supply 1 drew an average of 511.81W, while power supply 2 drew an average of 549.37W from the wall. Combining the draw from both power supplies, the total power drawn from the wall by the switch was 1061.17W, resulting in an overall switch efficiency of 79 percent.

PSE 6 CENTRALIZED

The second centralized switch system tested by the research team was the PSE 6 The same components connected to the PSE 3 were transferred to this switch for consistency in comparison (Table 33).

Table 32: Centralized Loading - PSE 6

PSE 6 24 Port - Centralized	**Quantity**	**Wattage (W)**
Luminaires	8	629.36
PoE Mini PCs	8	154.72
PoE PAC	4	47.16
PoE Cameras	4	15.2
PoE Wattage	**24**	**846.44**
Power Supply		1062
Total Consumed by the Switch		**1062**
Switch Efficiency		80%

The eight luminaires connected to the PSE 6 switch drew a combined 629.36W (78.7W each), while the PoE Mini PCs consumed a cumulative 154.72W. The PCs were configured to fully utilize CPU and

RAM resources as in the previous test, ensuring maximum power draw. The four PoE PAC and four PoE cameras drew a PoE power of 47.16W and 15.20W, respectively. The total PoE wattage consumed by all 24 devices was 846.44W.

The difference in PoE wattage between the PSE 3 and PSE 6 switches was 9.5W, or 1.13 percent, which can be attributed to the similarly sized loads on both switches. The PSE 6 switch features a dedicated rack-mountable 1U power supply unit which draws a total of 1062W from the wall. This results in a switch efficiency of 80 percent, which is nearly identical to the 79 percent efficiency observed in the PSE 3 switch.

DECENTRALIZED

For the decentralized architecture, the same four components previously tested in the centralized configuration—PoE PAC, PoE Cameras, Luminaires, and PoE Mini PCs—were redistributed across four separate switches based on the switch output and the expected load. The smaller loads, consisting of the PoE PAC and PoE Cameras, were tested on the PSE 1 switch, which has a maximum available PoE wattage of 120W. The larger loads, including the eight PoE Mini PCs and the eight luminaires, were tested on the PSE 5. Power consumption and wattage were measured using three different Xitron meters, and the efficiencies for each component-switch combination were calculated accordingly (Table 34).

Table 33: Decentralized Architecture - Loads on different switches

PoE PAC on PSE 1	Wattage (W)	PoE Cameras on PSE 1	Wattage (W)	Luminaires on PSE 5	Wattage (W)	PoE Mini PCs on PSE 5	Wattage (W)
PoE PAC 1	11.37	PoE Camera 1	3.34	Luminaire 1	76.58	Mini PC 1	19.38
PoE PAC 2	11.41	PoE Camera 2	3.64	Luminaire 2	78.2	Mini PC 2	19.68
PoE PAC 3	11.71	PoE Camera 3	3.66	Luminaire 3	78.24	Mini PC 3	19.07
PoE PAC 4	11.31	PoE Camera 4	3.06	Luminaire 4	76.76	Mini PC 4	18.26
Total PoE Power	45.8	Total PoE Power	13.7	Total PoE Power	619.56	Total PoE Power	152.78
Total System Power	63.94	Total System Power	28.68	Total System Power	813	Total System Power	222.33
System Efficiency	72%	System Efficiency	48%	System Efficiency	76%	System Efficiency	69%

Over the one-hour test period, the four PoE PACs consumed a total of 45.8W, while the four PoE Cameras drew 13.7W in total. The PSE 1 switch uses an external power brick, and the research team recorded wattage measurements both before and after the power brick. When the switch was powering the PoE PACs, the power brick efficiency—calculated as the ratio of DC power supplied to the PoE switch versus the AC power drawn from the wall—was 88.1 percent. For the PoE Cameras, the efficiency was 82.4 percent. These measurements indicate that the power conversion efficiency of the PoE switch's external power brick improves as the load increases.

The PSE 5 switch, which has a single power supply, was measured using a single channel of the Xitron meter. For the higher load, which included eight 90W luminaires, the total consumption for all eight units was 619.5W, while the power drawn by the PSE 5 power supply unit was 813W. For the eight PoE Mini PCs, the PoE consumption totaled 152.8W, with the power supply drawing 222.3W.

The smaller loads of the PoE Cameras and PoE PACs on the PSE 1 resulted in efficiencies of 48 percent and 72 percent, respectively. For the larger loads on the PSE 5, the efficiency was 69 percent for the PoE Mini PCs and 76 percent for the 90W luminaires.

To compare the efficiencies of the centralized and decentralized switch configurations, a weighted efficiency was calculated based on the decentralized efficiencies across the different switches handling various components (Table 35).

Table 34. Power Consumption and Efficiency of Decentralized Architecture

Component	Power Consumption (W)	Percent of Total Load (%)	Efficiency (%)	Weighted Efficiency (%)
PSE 5 – Mini PCs	152.8	18.3%	69%	13%
PSE 5- Luminaires	619.5	74.5%	76%	57%
PSE 1 – PoE PACs	45.8	5.5%	72%	4%
PSE 1 - PoE Cameras	13.7	1.6%	48%	1%
Total	**831.8**		--	**74%**

The decentralized system has been found to be less efficient than either centralized configuration. This is likely due to the redundant computational overhead of each individual switch in the decentralized architecture relative to the singular source of computational overhead in the centralized architecture (Table 36).

Table 35. Comparison of Centralized vs. Decentralized Efficiencies

Centralized vs Decentralized	
Total Weighted Efficiency for Decentralized System:	74%
Total Efficiency for Centralized System 1:	80%
Total Efficiency for Centralized System 2:	79%

Cybersecurity Evaluation

The first step in the cybersecurity analysis of each PoE system was a comprehensive review of the manufacturer's product documentations including spec sheets, installation manuals and best practices guides. The research team gathered all relevant product documentation by examining the provided documents, searching online, and directly reaching out to manufacturers, with a specific emphasis on cybersecurity-related materials.

In assessing the product documents, the research team developed a list of key specifications, configurations, and considerations expected to be covered in these documents, as described in the Methodology section. The team thoroughly reviewed each document, assigning scores across three categories:

- **Basic** - indicates that the topic was mentioned but only provided rudimentary or insufficient instructions.
- **Detailed** - signifies that the topic was comprehensively covered, providing enough information for an installer to properly install the system while avoiding cybersecurity vulnerabilities.
- **Not Present** – indicates that there was no mention of the specified topic in the documentation.
- **N/A** – indicates that the metric is not applicable to the specific device.

The goal of this effort was to determine if a manufacturer is providing all the relevant information necessary for an electrical installer to securely and safely install the products from a cybersecurity perspective. For each product, a more detailed analysis of the product documentation review and standards compliance can be found in the Appendix.

Table 36. Descriptions of electrical, physical and cybersecurity specifications examined in the product documentation.

Specification	Description
General Device Specifications	
PoE Requirements	Electrical specifications including voltage, current, and power consumption and PoE Standard
Network Interface Specifications	Details on Ethernet port speeds, compatibility, and connection types, protocols supported
Security Features	Built-in security capabilities like encryption support and intrusion detection

Specification	Description
Installation Procedures	
Secure Installation Practices	Best practices for safe handling, placement, securing device and network port access
Environmental Considerations	Guidelines on temperature, humidity, and electromagnetic interference
End Point Config/Hardening	
Changing default credentials	The ability to change factory-set usernames and passwords
Disabling unused services/ports	Turning off non-essential services and ports to minimize attack vectors
Firmware/Software Updates	Regular/automatic updates to patch vulnerabilities and improve functionality
Setting IP Parameters	Configuring static IP, subnet mask and gateway information
Network Config/Hardening	
Segmentation	Guidance on segmenting system from other IP networks, VLANs, subnets
Protocols Supported	Description of protocols used/supported in addition to PoE and IP
Securely Connecting to Network	Guidance on how to securely connect the device to an active network, air gapping
Switch Configurations	MAC limiting, DHCP snooping, port security, Dynamic ARP Inspection, etc.

In addition to the literature review analysis, a cybersecurity evaluation was conducted to assess the compliance of the devices with California Senate Bill 327 (Ca SB 327) and UL/ANSI 2900 standards. These standards outline essential security measures and authentication requirements for connected devices, to ensure their protection against unauthorized access and vulnerabilities. The research team utilized various tools from the Kali Linux suite to rigorously test multiple aspects of the devices' compliance with these standards, including tools like ‘slowhttptest’ for testing the devices' resilience to malformed inputs, brute force password cracking tools to assess password strength and protection, Nikto for vulnerability analysis, Nmap for port scanning and vulnerability assessment, and

Metasploit for testing potential exploitation of identified vulnerabilities, among others. The evaluation aimed to validate each device's adherence to these criteria, as detailed in Table 38 and Table 39. However, it is important to note that not all metrics could be validated for each device. In some cases, technical limitations prevented a thorough assessment, while in others, the lack of available information or access to necessary tools and software/firmware restricted the ability to fully evaluate compliance.

Table 37. Cybersecurity Compliance Criteria for SB 327

Category	Measure	Definition
Security Features	Appropriate Security for Device Function	Security measures must match the nature and functionality of the device to provide appropriate protection.
	Has appropriate security for handled information	The security features should safeguard the confidentiality, integrity, and availability of the data handled by the device.
	Has protection from unauthorized activities	Security measures need to prevent all forms of unauthorized interactions with the device and its data.
Authentication Features	Unique Preprogrammed Passwords	Devices must include a factory-set password that is distinct for every device to prevent mass exploitation.
	User-initiated Authentication Setup	If a unique password isn't used, the device should require users to configure their authentication mechanism upon initial setup.

Table 38. Cybersecurity Compliance Criteria for UL/ANSI 2900

Category	Measure	Definition
Malformed Input Testing	Normal Operation when subjected to malformed input. Product configured per manufacturer recommendation	Does not reset, hang, throws exception, loses connection, disclose info, becomes non-responsive
AAA	Has authentication system	Has authentication system for any info or management functions that could affect or alter security
	Authentication Time-out	Uses time-out or similar method to prevent perpetual authorization

Category	Measure	Definition
	Uses cryptographically secure authentication	Refer to UL 2900 Appendix B
	Generalized error messages for failed authentication	Should not give any clues as to why authentication failed
	Support the ability to set requirements for strength or length of credentials	Min password length of 6 characters, after 10 sequential authentication fails implement a time-out
	Protect against brute force attacks	Should prevent automated brute force authentication attempts
	Prompts to change default credentials	Should be a mechanism to change default credentials upon first installation with a notification
	Listing Users	Product shall support possibility to manage the list of valid user accounts by adding, removing or suspending accounts or updating authentication credentials
	Privileges and Permission	Product shall support assigning privileges and permissions to roles and credentials and enforce principle of least privilege for every authorized role or user
	Session Management	When auth is terminated, product shall ensure renewed session is authenticated prior to allowing access. Stored data from previous session should not be used during creation of new session
Remote Connection	Remote Communication	Product shall ensure integrity and authenticity of all data communicated over any remote interface
Sensitive Data	Cryptography for storing data	Product shall utilize approved cryptographic algorithms
	Cryptographic Variance	Product shall use separate cryptographic key for each service, operation or function
Product Management	Updates	Product shall be designed and implemented to allow for application of security updates
	Integrity of Updates	Product shall verify authenticity of software updates cryptographically

Category	Measure	Definition
	Logging	Product shall be capable of maintaining one or more logs of all security-related events
	Data Storage	Product shall store all security related logs in non-volatile memory and shall not allow non-privileged users to remove or change them
	Data Removal	Product shall allow for complete erasure of all configuration, sensitive and personally identifiable data

Manufacturer 3

The research team first reviewed the product documentation from the Manufacturer 3 system. Manufacturer 3 offers a variety of PoE enabled building devices as well as PoE conversion devices intended to bring PoE power and data to non-PoE native devices. The research team evaluated the documentation for the Manufacturer 3 PoE LED driver, USB hub (USBC), PoE Mini PC adapter for mini PCs. PoE switch (PSE 5, PSE 6) and the main controller (Manufacturer 3 Controller) from Manufacturer 3.

Data sheets, installation manuals and help guides were collected from the delivered product boxes, Manufacturer 3 website and directly from the manufacturer via an email request. An overview of the product documentation review can be seen in Table 40.

Table 39. Results From Analyzing Manufacturer 3 Product Documentation For Relevant Electrical, Physical and Cybersecurity Information

Specification	PoE Controller	PoE LED Driver	USBC	PoE Mini PC adapter	PSE 5, PSE 6
General Device Specifications					
PoE Requirements	Detailed	Detailed	Detailed	Detailed	Detailed
Network Interface Specifications	Detailed	Detailed	Detailed	Detailed	Detailed
Installation Procedures					
Secure Installation Practices	Detailed	Basic	Basic	Basic	Detailed

Specification	PoE Controller	PoE LED Driver	USBC	PoE Mini PC adapter	PSE 5, PSE 6
Environmental Considerations	Detailed	Detailed	Detailed	Detailed	Detailed
End Point Config/Hardening					
Changing default credentials	Not Present	N/A	N/A	N/A	Basic
Disabling unused services/ports	Not Present	Not Present	N/A	N/A	Not Present
Firmware/Software Updates	Basic	Not Present	Not Present	Not Present	Not Present
Setting IP Parameters	Not Present	Not Present	Not Present	Not Present	Not Present
Network Config/Hardening					
Segmentation	Not Present	Not Present	Not Present	Not Present	Not Present
Protocols Supported	Detailed	Not Present	Not Present	Not Present	N/A
Securely Connecting to Network	Basic	Not Present	Not Present	Not Present	Basic
Switch Configurations	Not Present	Not Present	Not present	Not Present	Basic

SUMMARY OF FINDINGS

The Manufacturer 3 product documentation provides detailed information on power requirements, network interfaces, and installation processes for PoE controllers and switches. However, it lacks critical cybersecurity guidance, such as securing network installations and configuring basic port security. While the product manuals offer electrical installation guidance, they do not address securing PoE devices from unauthorized physical access, as recommended by NIST SP 800-53. The lack of instructions for configuring default credentials and securing network endpoints exposes the system to potential vulnerabilities.

The cybersecurity evaluation revealed significant non-compliance with SB 327 and UL/ANSI 2900 standards. The Manufacturer 3 system lacks basic security measures, such as encryption, authentication, and secure user management. It does not handle malformed inputs well, making it vulnerable to attacks, and lacks mechanisms for software updates, cryptographic verification, and event logging. These deficiencies leave the system exposed to unauthorized access and data breaches.

Manufacturer 5 (PoE Camera)

Next, the research team gathered and examined the product documentation for the PoE Camera from Manufacturer 5. This effort included reviewing materials accompanying the physical device, searching the manufacturer's website, and directly contacting the manufacturer for information. The team located and analyzed a one-page product specification sheet along with a product manual. An overview of the product documentation review can be seen in Table 41. A more detailed analysis of the documentation review can be found in the Appendix.

Table 40. Results from Analyzing PoE Product Documentation For Relevant Electrical, Physical and Cybersecurity Information

Specification	PoE Camera
General Device Specifications	
PoE Requirements	Detailed
Network Interface Specifications	Detailed
Installation Procedures	
Secure Installation Practices	Basic
Environmental Considerations	Detailed
End Point Config/Hardening	
Changing default credentials	Basic
Disabling unused services/ports	Not Present
Firmware/Software Updates	Not Present
Setting IP Parameters	Not Present
Network Config/Hardening	
Segmentation	Not Present

Specification	PoE Camera
Protocols Supported	Detailed
Securely Connecting to Network	Basic
Switch Configurations	Not Present

SUMMARY OF FINDINGS

The PoE Camera product documentation provides details on power requirements, network interfaces, and protocols, including both secure (HTTPS) and insecure (FTP) options. However, the installation manual lacks crucial cybersecurity guidance, such as best practices for mounting to prevent tampering, hiding the PoE connection, and network security protocols like IP segmentation. Password guidance is also insufficient, recommending only a six character minimum.

The device partially complies with SB 327 and UL/ANSI 2900 standards. It uses strong encryption but lacks unique preprogrammed passwords, leaving it vulnerable to unauthorized access. Additionally, it fails to handle malformed inputs and uses outdated cryptographic methods (MD5), posing risks of denial-of-service attacks and weak password protections. Improved user management and secure data storage are also needed to meet compliance standards fully.

Manufacturer 7 (PoE Shades)

The next product documentation evaluated by the research team was that of the PoE enabled shades. Unlike the other products evaluated in this project, the PoE shades product did not come with any accompanying product information. The research time was also unable to find any product documentation on the Manufacturer 7 website. After reaching out to Manufacturer 7 support by phone, the research team received an installation guide as well as a user manual for the two different control software tools. The results from the product documentation review can be seen in Table 42.

Table 41. Results from Analyzing Manufacturer 7 PoE Shade Product Documentation For Relevant Electrical, Physical and Cybersecurity Information

Specification	PoE Shades
General Device Specifications	
PoE Requirements	Detailed
Network Interface Specifications	Not Present
Installation Procedures	

Specification	PoE Shades
Secure Installation Practices	Basic
Environmental Considerations	Not Present
End Point Config/Hardening	
Changing default credentials	Detailed
Disabling unused services/ports	N/A
Firmware/Software Updates	Not Present
Setting IP Parameters	Detailed
Network Config/Hardening	
Segmentation	Not Present
Protocols Supported	Not Present
Securely Connecting to Network	Not Present
Switch Configurations	Not Present

SUMMARY OF FINDINGS

The installation guide provides sufficient details on PoE power requirements and network setup, including IP addressing and user management. However, it lacks guidance on securing physical access to the PoE port and ensuring secure network integration. The software configuration tool offers useful features like network scanning and static IP assignment, aiding in network hardening.

The product documentation is deficient in cybersecurity guidance, particularly regarding physical security and best practices for securing network devices. The manuals fail to emphasize the importance of securing PoE connectors and switches, segmenting networks, and implementing switch configurations like port security and MAC address limiting.

Standards Compliance:

- **SB 327 Compliance:** The shade system fails to meet key SB 327 security requirements. It lacks unique credentials, allowing default passwords to be exploited. Additionally, it is vulnerable to replay attacks due to improper command hashing, and its encryption mechanisms do not fully protect data integrity.

- **ANSI/UL 2900 Compliance:** The system is non-compliant with key provisions. Although resilient to malformed inputs, it is vulnerable to denial-of-service (DoS) attacks and lacks a secure authentication framework. Weak encryption, no support for secure software updates, and the absence of logging and auditing further expose the system to potential attacks.

Manufacturer 8 (PoE AP)

The research team was able to find a product datasheet, an installation guide and many online tutorials and configuration guides for the PoE access point. These documents were collected from the manufacturer's website as well as from product literature that came with the physical devices. In addition to reviewing these documents, the team also conducted a hands-on cybersecurity analysis of the device to assess its practical security features and compliance with relevant standards. The results from the product documentation review can be seen in Table 43.

Table 42. Results from Analyzing Manufacturer 8 PoE AP Product Documentation For Relevant Electrical, Physical and Cybersecurity Information

Specification	PoE AP
General Device Specifications	
PoE Requirements	Detailed
Network Interface Specifications	Detailed
Installation Procedures	
Secure Installation Practices	Detailed
Environmental Considerations	Detailed
End Point Config/Hardening	
Changing default credentials	Not Present
Disabling unused services/ports	Not Present
Firmware/Software Updates	Detailed
Setting IP Parameters	Detailed
Network Config/Hardening	

Specification	PoE AP
Segmentation	Detailed
Protocols Supported	Detailed
Securely Connecting to Network	Detailed
Switch Configurations	Basic

SUMMARY OF FINDINGS

The product documentation provides detailed guidance for secure installation, covering PoE requirements, environmental factors, network interfaces, and physical security. The installation manual includes a "Pre-Install Preparation" section with steps to update firmware, set IP addresses, and configure firewalls. It also advises on physically securing the device, such as hiding CAT cables and using security screws. However, the manual lacks instructions for changing default credentials and WiFi settings, though these features are available within the device's configuration web interface.

Standards Compliance:

- **SB 327 Compliance:** The PoE AP shows strong compliance with SB 327. It enforces unique passwords during setup, uses modern encryption standards, and secures the device with password-protected access to its web interface. These measures help prevent mass exploitation and ensure secure communication.
- **UL/ANSI 2900 Compliance:** The device largely complies with UL/ANSI 2900, employing secure authentication protocols, strong password policies, and effective session management. However, the ability to handle all malformed inputs and store security logs in non-volatile memory could not be fully verified, leaving some areas of compliance uncertain. These gaps suggest potential vulnerabilities in high-security environments.

Manufacturer 9 (PoE PAC)

The PoE Access Control system is accompanied by extensive product documentation that can be found with the physical devices or on the manufacturer's website. The research team evaluated installation and configuration guides as well as product datasheets for each of the three devices evaluated: PAC Controller, PAC Hub and PAC Card Reader. The results from the product documentation review can be seen in Table 44.

Table 43. Results From Analyzing PoE Access Controller Product Documentation For Relevant Electrical,

Physical and Cybersecurity Information

Specification	PAC Controller	PAC Hub	PAC Card Reader
General Device Specifications			
PoE Requirements	Detailed	Detailed	Detailed
Network Interface Specifications	Detailed	Detailed	Detailed
Installation Procedures			
Secure Installation Practices	Detailed	Basic	Detailed
Environmental Considerations	Detailed	Detailed	Detailed
End Point Config/Hardening			
Changing default credentials	Not Present	N/A	N/A
Disabling unused services/ports	Not Present	Not Present	Not Present
Firmware/Software Updates	Basic	Not Present	Not Present
Setting IP Parameters	Not Present	Not Present	Not Present
Network Config/Hardening			
Segmentation	Not Present	Not Present	Not Present
Protocols Supported	Detailed	Not Present	Not Present
Securely Connecting to Network	Basic	Not Present	Not Present
Switch Configurations	Not Present	Not Present	Not Present

SUMMARY OF FINDINGS

The product documentation provides sufficient detail on PoE power requirements, network interfaces, and environmental considerations, as well as physical security guidance. However, key cybersecurity measures are lacking. The documentation does not cover methods to secure CAT cables or PoE ports for all devices, nor does it provide guidance on the necessary network security configurations or integration with other PoE switches. Although the companion app offers features like credential changes, IP address configuration, and firmware updates, these capabilities are not sufficiently highlighted in the installation manuals.

Standards Compliance:

- **SB 327 Compliance:** The PoE Access Control system complies with SB 327 standards, notably by eliminating default passwords and prompting users to create unique credentials during setup. The system secures data confidentiality and integrity using strong encryption methods, ensuring protection against unauthorized access.
- **UL/ANSI 2900 Compliance:** The system also aligns with UL/ANSI 2900 standards, with robust authentication mechanisms, secure communication protocols (HTTPS/TLS), and strong password policies. It enforces session management and protects against brute force attacks. However, some areas, such as handling malformed input and the storage of security logs, remain unclear, and the specific handling of cryptographic keys is undetermined.

Manufacturer 6 (PoE Vav)

The PoE VAV controller was not shipped with any accompanying product documentation. The research team was able to find a catalog sheet on the manufacturer’s website as well as installation and wiring best practices manuals after reaching out directly to the manufacturer. The evaluation of the product documents focused on identifying the presence of pertinent cybersecurity instructions relating to the product installation, with the results documented in Table 45.

Table 44. Results From Analyzing Manufacturer 6 PoE VaV Product Documentation for Relevant Electrical, Physical and Cybersecurity Information

Specification	PoE VaV
General Device Specifications	
PoE Requirements	Detailed
Network Interface Specifications	Detailed
Security Features	Not Present
Installation Procedures	
Secure Installation Practices	Not Present
Environmental Considerations	Detailed

Specification	PoE VaV
End Point Config/Hardening	
Changing default credentials	N/A
Disabling unused services/ports	Detailed
Firmware/Software Updates	Detailed
Setting IP Parameters	Detailed
Network Config/Hardening	
Segmentation	Not Present
Protocols Supported	Detailed
Securely Connecting to Network	Basic
Switch Configurations	Not Present

SUMMARY OF FINDINGS

The documentation for the PoE VAV controller provides comprehensive technical details on PoE power requirements, communication protocols (RS-485, BACnet IP, Modbus), and configuration of input/output ports via DIP switches. This flexibility allows installers to minimize potential attack surfaces by disabling unused ports. However, it lacks critical cybersecurity guidance, particularly concerning physical security, secure network integration, and PoE connections. The manuals do not address the use of managed switches or routers for enhanced security features like VLANs and access control lists, nor do they offer best practices for securing PoE connections, such as using properly secured PoE switches.

Standards Compliance:

- **SB 327 Compliance:** Evaluating the PoE VaV controller’s compliance with SB 327 was challenging due to its reliance on proprietary software. The device does not automatically acquire an IP address via DHCP, making it difficult to assess network-related security features. While it supports BACnet IP and firmware updates, the lack of accessible documentation and network interaction limits the evaluation of secure practices like cryptographic verification, changing default credentials, or enabling network security measures.
- **UL/ANSI 2900 Compliance:** The device’s limited interaction with standard network tools made it difficult to fully assess its compliance with UL/ANSI 2900 standards. Key aspects

like handling malformed inputs, session security, and encryption management could not be evaluated due to the need for PoE VaV's proprietary programming software.

Overall, while the PoE VaV controller may support some cybersecurity features, the reliance on proprietary tools and the lack of accessible network documentation hindered a full assessment of its compliance with SB 327 and UL/ANSI 2900 standards. Enhanced guidance on network security, managed switch usage, and secure PoE connections would improve the overall security posture of the device.

Penetration Testing

The following section outlines the penetration testing process for the Manufacturer 3 system under Architecture 1, where a single building system was installed on a single PoE switch, adhering to the manufacturer's recommendation. For this report, only one system within this architecture has been evaluated. Kali Linux, a comprehensive suite for cybersecurity auditing and penetration testing, was employed. The evaluation of remaining systems and architectures is scheduled for the next report.

Manufacturer 3 System Cybersecurity Analysis

SYSTEM ARCHITECTURE

The Manufacturer 3 Lighting system, comprising an 8-port PoE switch (PSE 5), a router/DHCP server, four PoE LED driver, and a Manufacturer 3 PoE controller, was subjected to a comprehensive penetration testing process (Figure 35). The system was configured following the manufacturer's guidelines. Each PoE LED driver was connected to the PoE switch via CAT5 cables, while the optical ports of the switch facilitated connections to a router (for DHCP service) and the PoE Controller (hosting the control webserver and applications). IP addresses are assigned to each PoE LED driver via the DHCP server on the default network space of the router (192.168.0.1/24). A network tap was placed in line between the PoE Switch and one of the PoE LED drivers to capture the data transmitted between the devices.

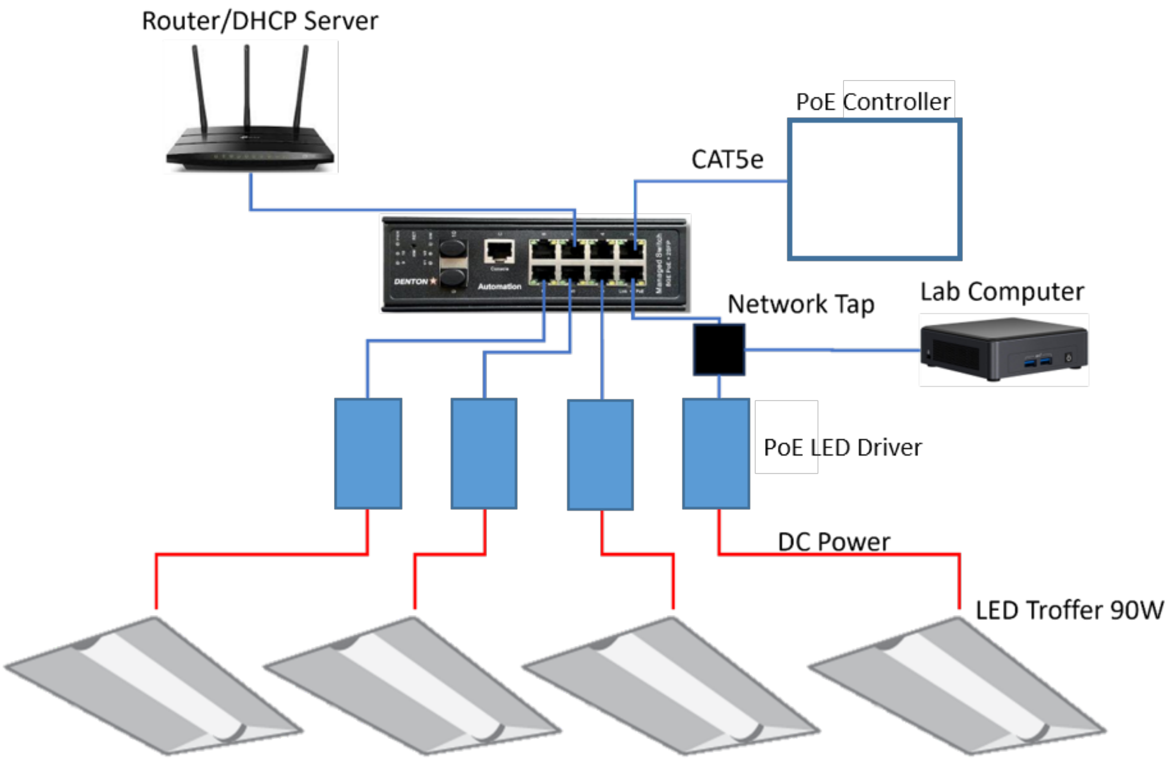

Figure 32: Network architecture for penetration testing of the Manufacturer 3 lighting system.

PACKET SNIFFING AND COMMAND DECODING

The PoE Controller hosts an HTTP webserver that allows the user to commission, configure and control the PoE end points through a web interface. To access the web interface, the user needs to be on the same network and must enter the IP address and port number of the PoE Controller into the URL bar of any web browser. There is no authentication system by default for accessing the PoE Controller's control web page. Additionally, the webserver uses the unencrypted HTTP, which leaves the data exchange between host and client vulnerable to capture. The first vulnerability identified was the lack of a default authentication system for the PoE Controller control computer. The control software can be accessed by any user on the same network that knows the IP address and port number of the web server, which can be determined with a network scan. The research team attempted to determine if there were other vulnerabilities associated with this control device and its method of communication.

In this first test, the research team monitored and logged the data exchange between the PoE Controller and PoE LED driver using Wireshark. The research team executed a variety of control commands from the PoE Controller to simulate real world usage of the lighting system. An analysis of the packet capture revealed that the control data was encoded but unencrypted. Commands such as dim, switch on/off and raise the light level were recorded and found to be consistent across all tests.

Similarly, the research team sent a variety of configuration commands from the PoE Controller to the PoE LED driver and also found these commands to be encoded but unencrypted. These configurations included commands to set the maximum wattage and the maximum allowable current, as well as setting the name for the PoE LED Driver. Finally, the research team captured the relevant IP parameters and port information for the PoE LED driver and the PoE Controller from this data stream.

After analyzing the packet capture, the research team devised two ways to control the PoE end points and the PoE Controller itself. In the first method, to gain access to the PoE network, the Lab Computer can either be connected directly to an open port on the PoE switch via a CAT5 cable or it can be connected to the switch by removing one of the PoE LED drivers and using its CAT5 cable. In a real-world setting, the latter approach might be more feasible as PoE switches are usually kept inside of locked IT rooms while an end point such as a PoE enabled luminaire might be more physically accessible. The Lab Computer will automatically receive an IP address via DHCP from the router as per the default network configuration recommended by the manufacturer. Additionally, since there are no port security measures in place on the switch, replacing the PoE LED driver with the Lab Computer on the network is possible. The research team created a script in Python to mimic the exact command packets that the PoE Controller sends to the PoE LED driver based on the packet capture data. To do so, the research team had to replicate the dataflow between the PoE Controller and PoE LED driver as seen in the figure below (Figure 36).

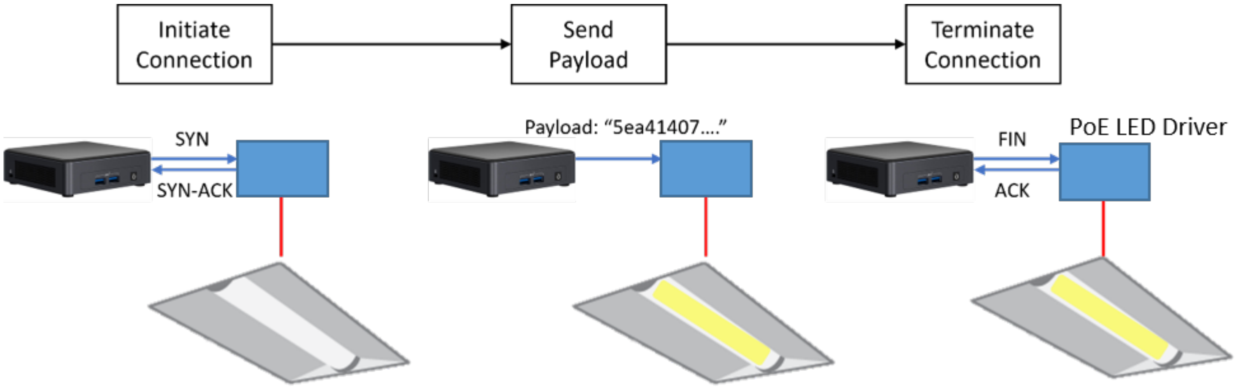

Figure 33. Dataflow for mimicking PoE Controller payloads to the PoE LED driver

Using this strategy, the research team was able to able to send valid control commands to any of the networked PoE LED drivers. It is notable that the PoE LED drivers will respond to a properly structured command, regardless of the source of the command. In the lab, the research team wrote a sample script that lowers the light level of all connected PoE LED drivers from 100% to 0% in increments of 10% before raising the light levels back to 100% in the same increments. It should also be noted that access to the network can be achieved without removing a device from the network if the PoE end point is the USB-C hub. This device is intended for user to connect USB-C devices such as laptop, smartphones and tablets, for both power and network connectivity. Without network and port security configurations, an attacker could use this USB-C device to gain access to the network while using the device as the manufacturer intended.

For the next test, the research team attempted to capture the commands sent between a user accessing the PoE Controller’s control web page and the PoE Controller itself. To do this, a network tap was placed in between the PoE Controller and the PoE switch and Wireshark was used to capture the packets (Figure 37).

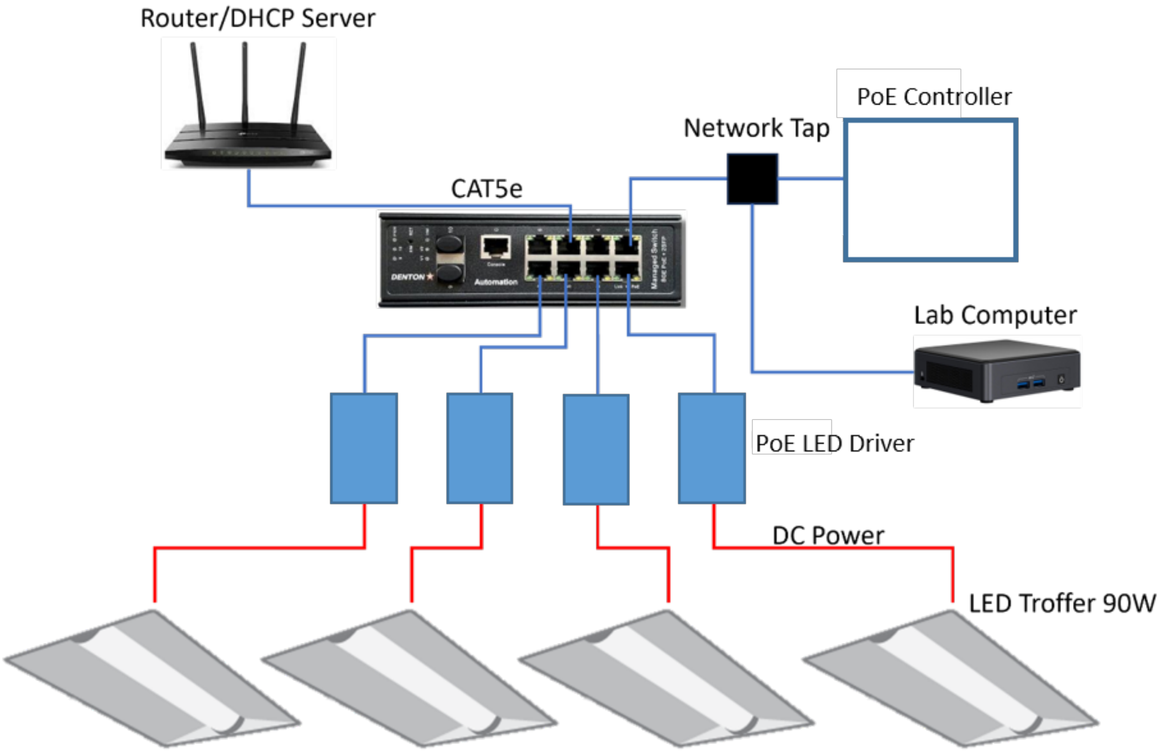

Figure 34. Network tap is placed between the PoE switch and the PoE Controller control computer to capture control commands

The research team accessed the PoE Controller's control web page from another networked computer and began navigating the user interface and issuing control commands to the connected PoE LED drivers. After analyzing the data, the research team was able to map out many of the PoE Controller's valid HTTP endpoints which allowed the team to create a script to replicate the functionality of the web interface programmatically from a remote computer. Since there is no authentication or encryption, simply sending the appropriate GET, POST or PUT command to the correct HTTP end point causes the PoE Controller to respond as if a valid user were manipulating the web interface. This script enabled the research team to manage and manipulate every feature of the PoE system that a user could via the web interface.

MAC FLOODING AND COMMAND DECODING

Finally, the research team attempted to capture and decode the control commands without the use of a network tap. For this attack, the research team disconnected one of the PoE LED drivers from the PoE switch and connected the Lab Computer (Figure 38).

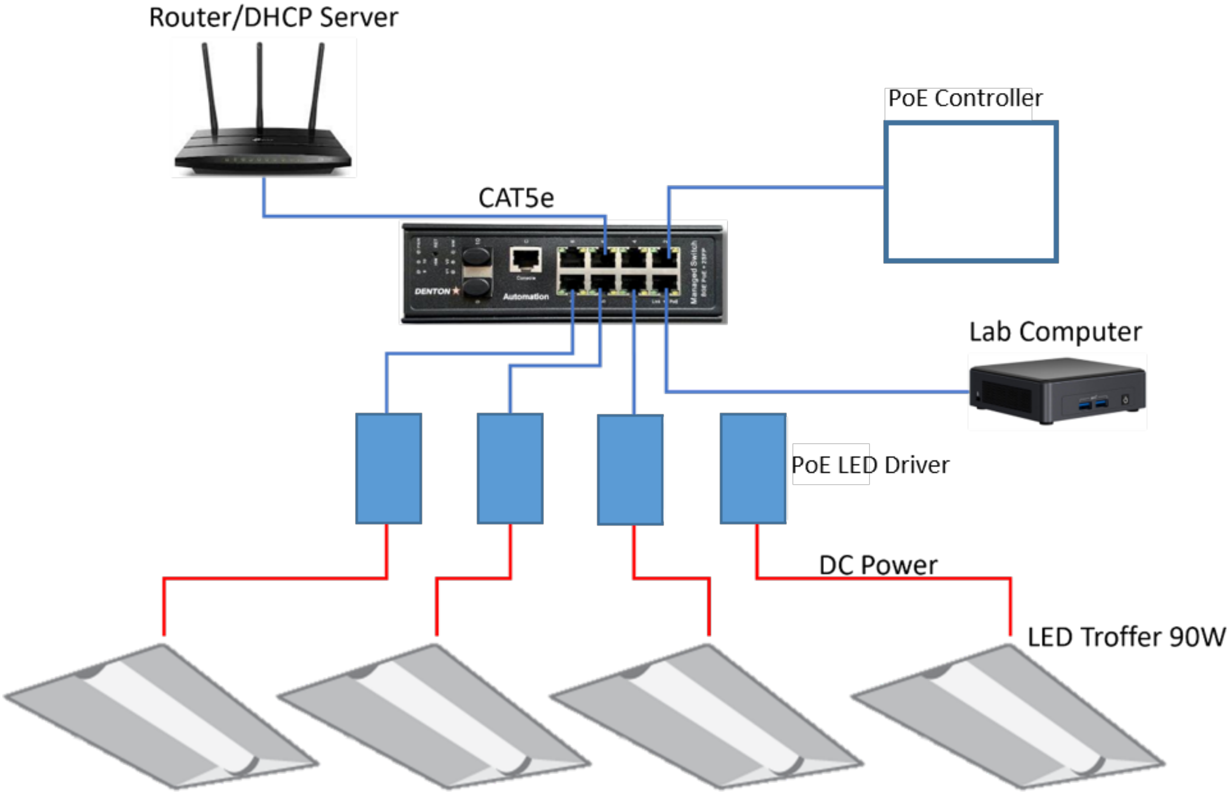

Figure 35. Network architecture for the MAC Flooding attack

Since there are no port security measures by default and the router is using DHCP, the Lab Computer is able to join the network in place of the PoE LED driver. From here, the team used the *macof* tool from the Kali Linux suite to begin the MAC flooding attack on the PoE switch. The goal of this attack is to send many Ethernet frames from different, spoofed, MAC addresses to the PoE switch in quick succession in an attempt to overflow the Content Addressable Memory (CAM) table. When the CAM table is filled, the switch loses the ability to map which MAC addresses are connected to which port. In this state, most switches in default configuration will revert to a fail-open mode where any incoming frame is broadcasted to all ports on the switch instead of just the intended target port thereby exposing all traffic through the switch.

Once the MAC flooding was complete, the research team used Wireshark to capture the control data from PoE Controller to the PoE LED drivers as before, but this time without the need for an inline network tap.

The penetration tests on the Manufacturer 3 system revealed vulnerabilities, particularly in the realms of data encryption and switch security configurations. The unencrypted data transmission between the PoE LED drivers and the switch presents a significant security risk, making the system susceptible to data interception and unauthorized control. Furthermore, the successful MAC flooding attack underscores the necessity for robust default security configurations on PoE switches.

It is, however, important to note some critical caveats. Firstly, these attacks largely presuppose that the attacker has physical access to the building and, in some cases, direct access to the PoE switch.

Such access scenarios should be improbable if proper physical security measures are in place to secure the PoE switch. Moreover, MAC flooding, a significant aspect of the penetration strategy, is unlikely to succeed on a switch that is actively monitored or correctly configured with contemporary security protocols. Furthermore, the strategy involving the replacement of a PoE LED driver with an attacker's computer should be thwarted by port security measures inherent in modern network switches. These measures prevent unauthorized devices from connecting to the network, rendering such an attack ineffective. However, port security configurations would not prevent an attacker from accessing the network through the USB-C hub device. Additionally, consolidating the PoE LED driver in a secure location, like a locked closet, and merely extending the DC power wires to the luminaires could significantly mitigate the risk of unauthorized physical access. This approach would limit potential attack vectors to the physical components of the PoE system, enhancing the overall security posture.

PoE Shades Cybersecurity Analysis

OVERVIEW

The PoE Shades are automated window shades that use Power over Ethernet (PoE) for power and data transmission. This system is designed to be energy-efficient and integrates seamlessly with PoE infrastructure. The Manufacturer 7 PoE shade system follows the industry standard (IEEE 802.3af/at) and works with regular PoE switches or injectors, consuming a maximum of 15.4 watts. The described setup for testing included an 8-port PoE switch, a router with DHCP server functionality, a Manufacturer 3 PoE controller, and several PoE shades. Each shade connected directly to the switch using CAT5 cables. The router provided DHCP services and internet access, while the PoE Controller hosted the control software. Finally, a network tap monitored the data flow between a switch and one of the shades (Figure 39).

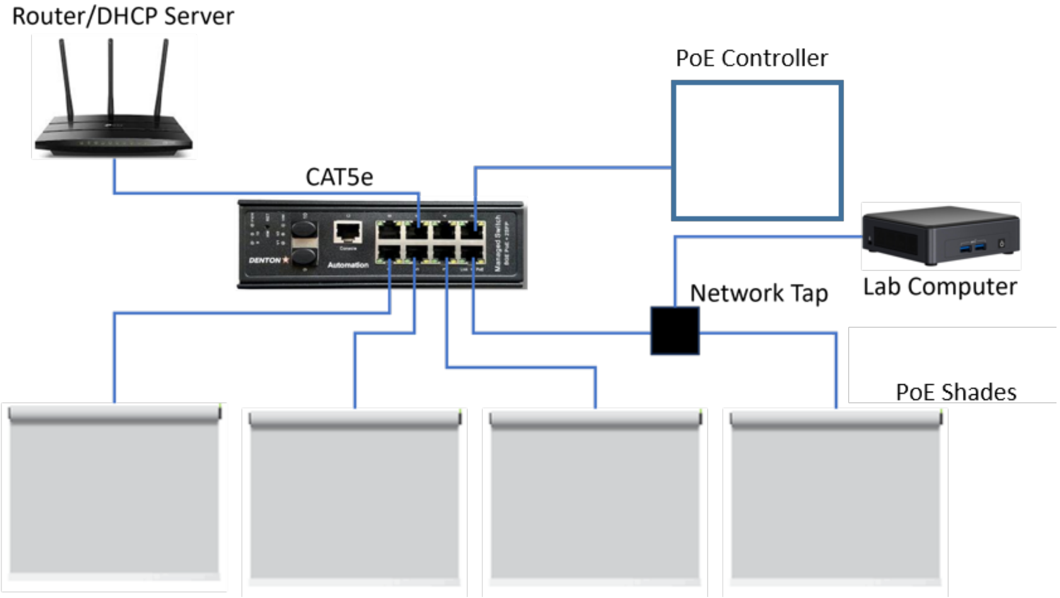

Figure 36. System architecture for the PoE shades

PoE shades utilize an encrypted communication protocol for transmitting control commands. Each command consists of a unique hash of the subsequent bytes, ensuring that only verified controllers with the private key can generate valid commands. This security measure is essential for preventing unauthorized control. However, the system has been found to have a critical vulnerability due to its implementation of the counter value in the message hash. Specifically, the PoE Controller software interacting with PoE shades does not increment the counter value, and the PoE shade device does not verify the counter's increment. This dual oversight simplifies the hash to a direct function of the motor position command, making the system susceptible to replay attacks where pre-recorded commands can be reused to control the shades.

VULNERABILITY ANALYSIS AND EXPLOITATION TECHNIQUES

To identify vulnerabilities, the research team first attempted to sniff the data transmitted between the PoE Controller and the PoE shaes. While the PoE shades can be controlled with their own standalone software, they can also be integrated into the Manufacturer 3 PoE environment. The data was sniffed by placing a network TAP inline with the shades, which allowed the capture of all traffic between the controller and the shades. Additionally, if direct access to the PoE shades is not possible, a MAC flooding attack on the PoE switch could fill the CAM table, causing it to operate in a fail-open mode, making all network traffic visible to an attacker.

Other potential attacks include ARP spoofing and VLAN hopping. ARP spoofing involves an attacker sending falsified ARP (Address Resolution Protocol) messages to a local network. This results in the attacker’s MAC address being associated with the IP address of a legitimate device on the network, enabling the attacker to intercept, modify, or block data intended for that device. In the context of PoE-enabled shades, an attacker could use ARP spoofing to intercept the commands sent from the PoE Controller to the shades, capturing the necessary data to replay commands.

VLAN hopping is another technique where an attacker manipulates network configurations to gain access to traffic on different VLANs (Virtual Local Area Networks). This can be done through switch spoofing, where the attacker tricks the switch into thinking their device is a trunk port, or double tagging, where the attacker sends packets with multiple VLAN tags. These methods allow the attacker to bypass network segmentation, gaining access to sensitive traffic, including the communication between the PoE switch and shades. Since PoE devices often share infrastructure with other network systems, VLAN hopping can expose the centralized control and data paths to unauthorized access.

Since the shades are PoE-enabled, the CAT cable used for both power and data transmission may be more accessible in public or less secure areas. This increased accessibility makes it easier for someone to place a TAP inline, further compromising the security of PoE-enabled devices like shades.

The research team placed a network TAP inline with the PoE shades and captured the communication packets between the PoE Controller and the PoE shades. By sniffing the packets corresponding to each possible shade position (0-100%), a hash table of position-hash pairs was created. This table allows for the manual control of the shades by replaying the specific hash values, effectively bypassing the intended security mechanism.

An example payload for moving the shades to the 0% position (fully down) is as follows:

Byte Position	00	01	02	03	04	05	06	07	08	09	0a
Data	x0a	x00	x6e	xb7	x1a	x00	x01	x00	x01	x00	x00

- x0a: Number of bytes after the initial 8 (10 in this case)
- x00: Undetermined, possibly padding
- x6e xb7: Unique hash of all subsequent bytes, within both the header and the rest of the command-specific payload
- x1a: Command code (1a is ‘move to %’)
- x00: Unique counter value
- x01: Undetermined
- x00: Undetermined
- x01: Undetermined
- x00: Undetermined
- x00: The % to move the motor to (in this case 0%)

The hash value `x6e xb7` changes with different position values but remains constant for the same command and position due to the flawed implementation.

MITIGATION STRATEGIES

Mitigating PoE-specific vulnerabilities associated with devices like PoE shades involves several strategic measures aimed at enhancing both network and device security. Firstly, it is crucial to address the counter value management issue. Ensuring that the controlling software increments the counter value for each command and that the PoE shade device verifies these increments will prevent replay attacks by ensuring that each command remains unique and cannot be reused maliciously. Additionally, implementing robust encryption protocols for all data transmissions between the controller and PoE devices, alongside mutual authentication methods, will significantly bolster the security framework, ensuring that only verified entities can communicate.

Network segmentation is another critical strategy. By employing VLANs to segment network traffic, sensitive data can be isolated, thus preventing unauthorized access through VLAN hopping attacks. Proper configuration and maintenance of these VLANs are essential to maintain the integrity of the network. Physical security measures are also vital; restricting physical access to network cables and PoE switches can prevent the unauthorized placement of network TAPs. Secure enclosures and access controls should be used to protect the physical network infrastructure, minimizing the risk of direct tampering.

Furthermore, the secure configuration of PoE switches is paramount. PoE switches should be configured to limit the number of MAC addresses per port, reducing the risk of MAC flooding attacks. Enabling security features such as DHCP snooping, ARP inspection, and port security can protect against various network spoofing attacks. Network monitoring tools and intrusion detection systems should be deployed to detect and respond to unusual network activities in real-time, thereby mitigating potential attacks as they occur.

Regular firmware and software updates are essential to address known vulnerabilities and implement the latest security patches. Manufacturers should be encouraged to provide timely updates and continued support for their products. Finally, educating network administrators and installers on the best practices for securing PoE networks is crucial. Training should encompass proper configuration techniques, recognizing potential vulnerabilities, and implementing robust security measures to ensure the overall security of PoE-enabled systems.

By integrating these measures, the security of PoE-enabled devices like shades can be significantly enhanced, reducing the risk of unauthorized access and control, and ensuring a more secure and resilient network infrastructure.

Discussion and Conclusion

The comparative analysis of Power over Ethernet systems and traditional AC/DC power supplies provides significant insights into the efficiency and application suitability of these technologies. This discussion collates the key findings to guide decision-making regarding the selection of power delivery methods and switches in various scenarios.

PoE vs. AC/DC Power Efficiency

One of the primary takeaways from this analysis is the consistently higher efficiency of AC/DC power supplies compared to PoE systems. For example, the PoE camera demonstrated an efficiency of 84% when powered by an AC adapter, significantly outperforming the 37-41% efficiency observed when using PoE switches. The main factor contributing to this efficiency gap is not merely the line losses or DC-DC conversion within the device, but rather the substantial power consumption and overhead of the PoE switch itself.

In the case of the PoE cameras, the PoE switch consumed an additional 20.2W just to power four cameras, while the cameras themselves only drew a total of 14W (3.5W per camera). In contrast, when powered by individual AC/DC power bricks, each camera required just 2.86W of DC power, with the power adapter itself drawing only 3.42W from the wall. This means the AC/DC adapter added just 0.56W of overhead per camera, totaling only 2.24W for all four cameras. Thus, the PoE switch's 20.2W overhead is nearly 10 times greater than the combined 2.24W overhead of the four AC/DC power bricks, highlighting the much higher efficiency of using traditional power supplies over PoE in this scenario.

Furthermore, the cameras required less DC power (2.86W) when powered by the wall bricks compared to when powered by the PoE switch (3.5W). This suggests that the DC output of the wall brick is closer to the actual power requirements of the camera, minimizing unnecessary energy loss. In contrast, the PoE switch provides a higher voltage to the camera, which then requires additional DC-DC conversion within the device, leading to further inefficiencies and greater energy loss.

When examining higher-power devices like LED luminaires, the Manufacturer 3 PoE LED driver system demonstrates how higher loads can lead to increased AC/DC conversion efficiency. This aligns with the hypothesis that higher loads on a PoE system can reduce the relative impact of the switch's overhead, leading to greater efficiency. In the case of the luminaires, the PoE system achieved an efficiency of 80% when heavily loaded, which is notably better than the efficiency observed in lower-load scenarios like those with the PoE cameras.

A key point in this analysis is that the PoE node, which serves a similar role to the AC LED driver by providing constant current power to the LEDs, was itself highly efficient at 92%. Unlike the Meanwell driver, which is an AC-constant current DC supply, the PoE node functions as a DC-constant current DC supply. This high efficiency of the PoE node underscores that the main source of inefficiency in the PoE system is the PoE switch, not the node.

Even with the improved efficiency at higher loads, the PoE system still lags behind the traditional AC/DC architecture. The AC/DC driver powering the same luminaires reached an efficiency of 91%, demonstrating that while higher loads can reduce the relative impact of the PoE switch’s overhead, the switch’s inefficiency still results in a lower overall system efficiency compared to the AC/DC solution.

The comparison between PoE and traditional AC/DC power systems highlights the persistent inefficiencies inherent in PoE setups, particularly due to the power consumption and overhead of the PoE switch. Even when higher loads improve conversion efficiency, PoE systems still lag behind AC/DC solutions in overall efficiency. Understanding the role of the PoE switch is critical to optimizing these systems, as it significantly impacts energy performance.

Switch Efficiency

The analysis of various PoE switches offers valuable insights into their efficiency under different loading conditions, highlighting both their strengths and limitations compared to traditional AC-powered devices. While PoE technology provides significant benefits, such as centralized power management and reduced infrastructure complexity, the data indicates that PoE switches generally exhibit lower overall system efficiencies than traditional AC-powered systems, particularly under certain load conditions.

One of the key takeaways from the data is that PoE switches tend to perform most efficiently at mid-range loads, typically around 60-70% of their total capacity. This was particularly evident in switches like the PSE 1 and PSE 2, which showed peak efficiency within this range. However, even at their optimal performance, PoE switches generally do not achieve the same efficiency levels as traditional AC-powered devices. This suggests that careful consideration of the expected load range is crucial when deploying PoE systems, as operating outside of the optimal load range can exacerbate inefficiencies.

High-capacity switches, such as the PSE 3 and PSE 6, demonstrated consistent efficiency across a broader range of loads, particularly excelling under higher load conditions. These switches are well-suited for environments with substantial and fluctuating power demands, where their ability to manage large loads with stable efficiency is beneficial. However, it is important to note that their efficiency still falls short of that achieved by AC-powered systems, even when fully loaded.

In environments with mixed loads—where large loads like luminaires coexist with smaller loads such as access controllers—or where loads vary over time, such as lights that dim or turn off, switches that maintain stable efficiency across a variety of load conditions are particularly advantageous. The PSE 3 and PSE 6 excel in these scenarios due to their versatility and consistent performance across both varying and mixed loads, making them ideal for dynamic, mixed-use applications.

For smaller, consistent loads, such as security cameras that require continuous power but may draw less than the minimum PoE power specification of 15W, switches like the PSE 4 8-Port are effective due to their relatively higher efficiency at lower load percentages. This makes them suitable for powering smaller devices that need to remain operational at all times, although they may still not match the efficiency of traditional AC solutions in these cases.

Overall, the data underscores the importance of selecting the right PoE switch based on the specific load conditions expected in the deployment environment. While PoE systems offer valuable advantages in terms of centralization and infrastructure simplification, traditional AC-powered systems may still be preferred in scenarios where maximizing efficiency is the primary concern.

Centralized vs. Decentralized PoE Architectures

The study also compared centralized and decentralized PoE architectures, revealing that centralized systems exhibit better efficiency under the conditions tested. The centralized systems, using large switches like the PSE 3 and PSE 6, achieved efficiencies of 79-80%, outperforming the decentralized systems, which had an overall efficiency of 74%. This suggests that centralized PoE systems are more efficient, particularly in environments with diverse power demands, where a single large switch can manage multiple loads more effectively than several smaller switches.

In addition to this, the decentralized configuration suffers from the cumulative overhead of each individual switch. Each PoE switch has an internal computer or controller responsible for managing its functionality, which introduces computational overhead. In a centralized configuration, this overhead is diluted across the entire load, minimizing its impact on overall efficiency. However, in a decentralized setup, this overhead is replicated for each switch, leading to a compounding effect that further reduces efficiency. This redundancy in computational overhead contributes to the lower efficiency observed in decentralized PoE systems, making centralized architectures a more efficient choice for large-scale deployments where minimizing energy consumption is critical.

The cybersecurity assessment of various PoE and AC-powered devices revealed notable differences in security practices, vulnerabilities, and compliance with key standards, such as California Senate Bill 327 (SB 327) and UL/ANSI 2900. The analysis highlights both successes and significant gaps in the cybersecurity implementation of these systems, providing valuable insights into the current state of device security and the critical areas where improvements are needed.

Standards Compliance and Security Implementation

Across the devices tested, compliance with SB 327 and UL/ANSI 2900 cybersecurity standards was inconsistent. While some devices, such as the PoE Access Control system and PoE Access Point, exhibited strong compliance with authentication and encryption requirements, others, such as the Manufacturer 3 devices and PoE shades, demonstrated significant shortcomings in basic security features. For instance, devices like PoE shades and PoE LED driver lacked critical features like encryption, robust authentication mechanisms, and secure firmware update capabilities, rendering them vulnerable to unauthorized access and manipulation.

Authentication and Encryption Gaps

A recurring issue across many devices was the lack of unique preprogrammed passwords and insufficient enforcement of password complexity. For example, the PoE camera lacked unique default passwords, leaving the system exposed to exploitation via common default credentials. Additionally, it did not protect against automated brute force login attempts, as it had no timeout or rate limiting for failed login attempts. Devices such as Manufacturer 3 system and PoE shades exhibited weak or incomplete encryption implementations, making them susceptible to replay attacks and data interception. The absence of these fundamental security features highlights a broader challenge: manufacturers often provide limited guidance on implementing strong authentication and encryption protocols, or fail to enforce them by default.

In contrast, devices like the PoE Access point and PoE Access Control system excelled in this regard, offering strong encryption protocols (e.g., HTTPS, TLS) and requiring secure password configurations at setup, which significantly reduces the risk of unauthorized access. These devices also demonstrated good practices for session management, protecting against brute force attacks by enforcing timeouts after multiple failed login attempts.

Vulnerabilities in Input Handling and Network Management

The evaluation also uncovered vulnerabilities related to handling malformed inputs and managing network configurations. Devices such as the PoE camera failed to handle malformed HTTP requests properly, leading to system crashes that could expose them to denial-of-service attacks. Similarly, PoE shades demonstrated weaknesses in its cryptographic functions, allowing for potential replay attacks due to the improper implementation of message hashing mechanisms.

Documentation Gaps and Manufacturer Guidance

One of the critical findings of this assessment is the significant variation in the quality and comprehensiveness of manufacturer-provided documentation regarding cybersecurity measures. Many manufacturers failed to provide sufficient detail on secure installation practices, firmware updates, or device hardening techniques, leaving installers and system administrators to configure devices with limited guidance on securing them against cyber threats.

For example, while the PoE Access Control system included detailed instructions on securing physical and network access, devices like PoE shades and the PoE LED driver provided only basic or incomplete information on network security practices. This inconsistency points to the need for manufacturers to prioritize cybersecurity guidance in their documentation, particularly for devices intended to be integrated into larger networked systems.

Implications for System Security and Design

The combined results of the cybersecurity assessment and electrical performance analysis highlight several important implications for the deployment, management, and optimization of networked devices:

1. **Prioritize Security and Efficiency in System Design**: System designers must evaluate both the cybersecurity features and energy efficiency of devices before deployment. Devices with strong encryption, authentication, and update mechanisms should be prioritized, as those lacking these features, such as the PoE camera with weak brute force protection or Manufacturer 3 system and PoE shades with incomplete encryption, can become significant vulnerabilities. Likewise, when efficiency is critical, AC/DC power systems are often

preferable for stationary, high-load devices where power electronics can be tailored to maximize performance.

2. **Comprehensive Documentation and Installation Guidance**: Manufacturers should provide not only detailed electrical safety and installation instructions but also thorough cybersecurity guidance in their documentation. Just as proper electrical installation ensures the safety and functionality of PoE systems, relevant cybersecurity information is essential for protecting these networked devices from malicious attacks. PoE technology, while offering convenience, centralized management, and controllability, also introduces inherent cyber vulnerabilities by significantly expanding the threat surface through the addition of many more IP endpoints. Without clear guidance on changing default credentials, securing network ports, and implementing network segmentation, these devices could be left exposed to unauthorized access and data breaches. It is crucial that manufacturers explicitly communicate these risks and provide mitigation strategies to installers. This will ensure that PoE systems are not only installed correctly from an electrical perspective but also secured from a cybersecurity standpoint. Proper documentation that addresses both aspects comprehensively will help maximize the efficiency and security of PoE deployments, making them safer and more resilient for long-term use in connected environments

3. **Optimizing System Performance with Proper Device and Switch Selection:** While PoE systems offer advantages like centralized power management and simplified installation, their efficiency can be hindered by the overhead power consumption of PoE switches. The selection of appropriate switches and careful load management are critical to improving overall system performance. Our findings show that certain PoE switches, such as the PSE 2, operate most efficiently at more fully loaded conditions, while others, like the PSE 3, maintain relatively stable efficiency across a wider range of loads. When designing a PoE system, it's essential to consider the types of loads being connected. Devices with constant power requirements, such as security cameras, will behave differently than those with varying loads, like dimmable lighting systems, which can affect the system's energy performance. The choice between **centralized** and **decentralized** architectures also plays a key role in system design. Decentralized systems, where separate switches power distinct subsystems, offer inherent cybersecurity benefits by physically segmenting systems, reducing the risk of lateral movement in case of a breach. However, these configurations often suffer from reduced electrical efficiency due to the overhead introduced by each additional PoE switch. In contrast, centralized architectures can offer better overall electrical efficiency by concentrating loads on fewer, larger switches, but require robust network security measures to mitigate the risks of lateral movement across the network. Implementing practices like VLAN segmentation and access control on centralized switches can help secure these systems while optimizing performance.

4. **Network Hardening Practices:** To protect networked devices, strong network hardening measures such as VLAN segmentation, port security, and access control are critical. Without these practices, even devices with good authentication and encryption protocols remain vulnerable to network-based attacks. Documenting and implementing these security measures alongside optimizing energy use creates a more robust and efficient system.

The findings from both the electrical performance and cybersecurity assessments provide a comprehensive framework for selecting and managing power delivery and network security for modern systems. AC/DC power supplies tend to offer superior efficiency, particularly for high-load, stationary devices where precise power requirements can be met. However, PoE systems present significant operational advantages in scenarios where ease of installation, centralized management, and reduced infrastructure complexity outweigh the efficiency losses inherent in these systems. From a cybersecurity standpoint, it is critical to prioritize devices with robust authentication, encryption, and update mechanisms while implementing network hardening practices to mitigate vulnerabilities. Additionally, the efficiency of PoE systems can be optimized through careful switch selection and load management. Ultimately, the design of a building system should balance the specific needs of the application in terms of efficiency requirements, installation costs, and controllability. However, cybersecurity should always be a foremost consideration in all implementations. The insights from this analysis provide a practical framework for making informed decisions that not only optimize electrical performance and installation convenience but also ensure robust security measures are integrated from the outset.