U.S. DEPARTMENT OF ENERGY

Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

Cyber Security for Lighting Systems

Lighting control systems have become more sophisticated having developed from wall switches to advanced controls that are network connected. These new systems are part of the facility related control systems (FRCS) and can be at risk for a cyber attack. These attacks can potentially affect the lighting system and also be a vector to attack other information technology (IT) systems.

This fact sheet focuses on the cyber threats unique to lighting control systems in buildings, and helps facility managers identify the types of lighting control systems that may introduce cyber security risks.

For more details on cyber protection refer to the Federal Energy Management Program (FEMP) *Facility Related Control Systems* fact sheet. https://www.energy.gov/sites/prod/files/2018/01/f46/cyber_securing_facilities.pdf

Light fixtures combined with certain types of sensors have cyber security risks.
Photo credit Pacific Northwest National Laboratory.

Lighting Controls Overview

In order to provide improved energy and operational efficiency, some federal facilities are incorporating connected or Internet of Things (IoT) lighting devices into building systems.

The terms smart, connected, IoT, Industrial Control System, and Operational Technology (OT) are similar (though not all synonymous) and typically refer to devices that provide features and communication abilities beyond legacy sensors. Major cyber security concerns relate to devices with an Internet Protocol (IP) address and communicate outside the building. Today only a few components of lighting equipment have IP addresses, but in the near future the number of devices with IP addresses is expected to triple or quadruple. It is anticipated that most equipment will be largely IP based.

Smart or connected lighting systems without an IP address communicate with other devices within the building. Physical security helps secure these systems because a person has to be in the facility to attack these systems.

Wired vs. Wireless

When designing a lighting system, one key early decision involves deciding between wired or wireless connection methods between light fixtures to controls, or controls to controls.

Wired

Legacy wired communication protocols (e.g., Building Automation and Control [BACnet]) have virtually no security mechanisms. The reason is that the wires are within the building and behind physical structures helping secure the wires. However, industry has started to develop secured versions of existing protocols because new functionality places them at risk.

New fixtures with a shared power and data cable including Power over Ethernet, distributed low-voltage power, and other similar technologies utilize IP addresses. Thus these systems have greater cyber security requirements than legacy control systems.

Wireless

Wireless devices require a low level of energy to operate, and power demands increase when encryption is introduced to help secure the system. There are different strengths of encryption: at a minimum Advanced Encryption Standard (AES) 128-bit encryption should always be employed for wireless devices. Stronger forms of encryption (i.e., AES 256-bit) exist but have power demands that limit their use on most current wireless smart devices.

After encryption, authentication, which limits unauthorized access to the system, is key to cyber security. Authentication establishes identity, verifying that the device sending the command is from a trusted source. Strong authentication involves both a public and private key, which is unique digital code. The public key initiates communication between the two devices. The authenticating device challenges the device being authenticated and the device being authenticated responds to the challenge with the private key. Authentication methodology is not currently listed on data sheets and needs to be verified with the specific technology manufacturer.

Risks

Table 1 provides an overview of lighting control systems and associated cyber security risk. Many control solutions pose little risk, but that risk increases with advanced lighting controls that are network or internet connected. Many common or legacy sensors pose little cyber risks. Table 2 provides a review of lighting controls, strategies and the related cyber security risks.

Commissioning/Configuring Risks

Commissioning is the process of configuring and verifying that the lighting system is performing as desired. Manufacturers have reduced commissioning complexity and costs by developing tools that use common wireless protocols incorporating wireless methods of commissioning via handheld devices. The cyber security risk of these wireless systems can vary from low to high risk depending on how they operate.

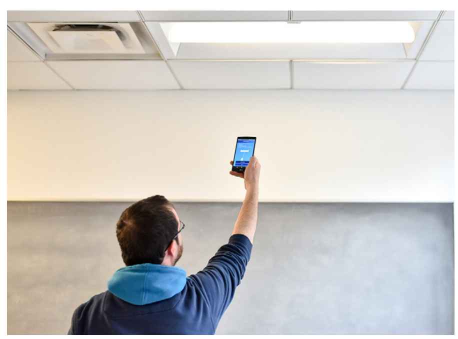
Typical wireless communication protocols for commissioning include infrared, Bluetooth Low Energy, visual flashing, near-field communication or Zigbee. The recommended best practice is to utilize these new commissioning devices for setup and configuration, but the sensors should be turned off after commissioning. Unauthorized use could result in inadvertent or intentional changes to operation of the system.

Table 1. Review of Light Fixtures and Associated Cyber Security Risk

Light Fixture	Description	Cyber Security Risk
Simple (no controls)	Light fixtures that turn on/off with switch or circuit breaker.	None
Light fixture connected to local lighting control	Light fixtures wired via a relay and power source to a local sensor (daylight or occupancy), wall dimmer, or timer.	None
Standalone fixtures with integrated controls, or non-integrated intelligent lighting controls	New light fixtures or retrofit kits with integral occupancy sensors and/or daylight sensors. Most fixtures or retrofit kits with integral sensors are constrained to controlling only that fixture that holds the sensor.	Low to moderate
Integrated lighting control	Systems that include local switches, sensors, and relays that are connected to a network and integrated to larger facility-related control systems.	Low to moderate
Integrated lighting control with network and Internet connections	New light fixtures or retrofit kits with integral occupancy sensors and/or daylight sensors with wired or wireless communications. These systems may connect to the building network and externally outside of the building to the cloud.	Moderate to low
Integrated lighting control with Power over Ethernet (PoE) or similar digital low voltage	New fixture options that get both their power and control communications through networked cables (e.g., Cat 5 or 6). The risk exists if the communication system is compromised.	Moderate to low

Commissioning can occur via a handheld device using a variety of different connectivity methods.

Modules inserted into the light fixture may be commissioned via a plug-in feature with a handheld device and then inserted into the light fixture.



During commissioning, light fixtures might be grouped to a sensor, the output settings of the fixture may be set, or other features set.

Photo credit Next Generation Lighting Systems, US DOE Solid-State Lighting Program

Table 2. Common Lighting Controls/Strategies and Associated Cyber Security Risk

Lighting Controls and Strategies	Description	Cyber Security Risk
Occupancy / Vacancy Sensors	Occupancy sensors automatically turn on/off lighting with movement in the space. Vacancy sensors allow for manual on/auto off. Traditional occupancy sensors detect movement via passive infra-red, ultrasonic, and microphonic sensors. Some retrofit options allow for wireless occupancy sensors. The sensors communicate with a relay that operates the fixture via wireless signal. There is no "smart" capability to these types of sensors and therefore no cyber risks.	None
	New sensors related to occupancy can count the number of people in the space. These sensors might use low resolution digital video sensors or other sensor types. Low resolution video requires the processing of data. If this processing occurs via the cloud or data stored in the cloud, cyber security risk increases.	Moderate
Daylight Harvesting	Daylight harvesting is the reduction of electric lighting in response to available daylight via a photocell. Typically these are stand alone systems where the photocell integrates with the light fixture(s) and there is no smart capability.	Low
	Some daylighting systems are advertising IoT with the additional features and capabilities from IoT-enabled daylight sensors. If the daylighting system is "connected" or IoT-enabled, cyber security risk increases.	Moderate to high
Tuning	Tuning is reducing (dimming) the light output to meet occupant needs or preferences. Many new lighting systems allow the lighting in workstations to be customized via tuning. The tuning occurs during commissioning and if the commissioning process involves a communication protocol that does not leave the building, the risk is low to moderate.	Low to moderate
	Some tuning systems utilize a cloud or external interface (e.g., log in via a website) to tune. The outside communication or interface increases the cyber security risk.	Moderate to high
Other Energy Benefits	New systems allow for sensors that might be integrated in the light fixtures to communicate directly with other building systems (e.g., HVAC, plug loads). Some of these sensors operate on low band wireless (e.g., 900 MHz), and thus wireless connectivity; the cyber risk is low.	Low
	Systems utilizing data from the sensors and sharing or processing via the cloud or other web interfaces may assist with energy management. Once the system connects outside the building, the risk increases.	Moderate to high
Interfacing with Building Automation Systems	Lighting controls can and often do interface with building automation/ management systems via wired and wireless communication methods. As OT systems become interconnected (which is desirable), each connected system increases the cyber security risk.	Moderate
Non-Energy Benefits	Non-energy benefits (NEBs) can offer added value from OT systems. Sensors related to NEBs could include sensors for tracking assets, measuring temperature, assisting with space utilization. Sensors for NEB virtually always require use cloud analysis or cloud data storage increasing cyber security risk.	Moderate to high

Attacks on Connected Lighting

Potential forms of attack on connected lighting systems include vectoring, distributed denial of service, sniffing, and privacy concerns.

Vectoring

Vectoring occurs when an intruder enters one unsecured networked system to gain access to other systems via the network.

Securing systems, encryption, authentication, and using air gaps between critical systems can limit vectoring.

Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. Examples exist of lighting technologies being used in DDoS attacks, however, these tend to be residential type products (e.g., WiFi-enabled light bulbs).

Before connecting a lighting device with an IP address to a network, consult your facilities information technology (IT) department. IT departments might test the device before allowing its use.

Sniffing

An attacker could see a packet (a unit of data) in transmission from one point to the other in systems that utilize protocols that are not encrypted. Because the packet is not encrypted, the information in the packet (e.g., lighting output value) could be maliciously modified by the attacker (e.g., turning off the lights in a government office).

First seek out an encrypted system. If the system is not encrypted, incorporate a virtual LAN (VLAN) between the light fixtures and gateways or network switches.

Privacy Concerns

Invasion of privacy is a concern related to connected lighting, because some new occupant detecting sensors utilize To address privacy concerns, these systems may utilize very low resolution camera technology to differentiate between a person and a computer, but low enough resolution that the camera could not successfully differentiate between two people.

Testing Programs

Cyber security is a combination of diligent planning, active management/monitoring, and the selection of the appropriate equipment. As part of product selection, testing the hardware and software used in the connected lighting systems is advisable.

National Testing Labs

National testing labs (e.g., UL, Intertek, ETL, CSA) test equipment for electrical, fire, and physical safety. Most people are familiar with these logos on the label of equipment. Many of these testing labs now offer cyber security testing services.

American National Standard Institute (ANSI)/UL 2900 is a series of standards providing measurable criteria for the testing of network-connected devices that send, store, or transmit data to/from networked devices. UL 2900-1 focuses on cyber security for appliances including lighting.

UL Cybersecurity Assurance Program, Intertek, and other testing labs can test product software for vulnerabilities, analyzes source code, robustness testing for all external interfaces and communication protocols, and limited penetration testing.

FedRAMP

Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud product services. FedRAMP allows users to search by product manufacturer or agency that has used the product.

Incentive Programs and Cyber Security Testing

The DesignLights Consortium (DLC) technical requirements for lighting, connected lighting, and controls are often the basis for rebates from utilities and energy efficiency programs. DLC is also referenced in lighting sections in federal design standards (PBS-P100 and UFC 3-530-01). The DLC is revising the Networked Lighting Control System Technical Requirements to incorporate cyber security requirements (current draft version 3 includes ANSI/UL 2900-1). Although, not a federal requirement, sites might need to use ANSI/UL 2900-1 lighting products to qualify for a rebate.

Summary

New connected lighting systems offer exciting improvements in energy and operational efficiencies, but care must be taken to ensure that they are cyber secure. As with legacy lighting systems, ensuring physical security is important. Devices with an IP address are at the greatest risk. This risk can be mitigated by utilizing 128-bit encryption or VLANs to secure equipment communications, and by selecting equipment with good authentication measures. Turning off sensors used to commission lighting systems once commissioning is complete is also important. For more sophisticated systems with advanced controls, such as PoE and systems that utilize the cloud, increased risk can be mitigated by following FEMP facility related control system guidance and product testing. ■

U.S. DEPARTMENT OF ENERGY
Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

FEMP
Federal Energy Management Program

For more information, visit:
energy.gov/eere/femp

PNNL-SA-134890 · May 2018