This document is intended for Lighting Control Systems and IT professionals

**Important:** Engage appropriate network security professionals to ensure all lighting control system hardware and servers are secure for access.

Network security is an important issue. Typically, the IT organization must approve configurations that expose networks to the Internet. Be sure to fully read and understand customer IT Compliance documentation.
Table of contents

Network and IT Considerations .............................................................. 3
WaveLinx Network Topology Options .................................................. 3
Dedicated WaveLinx .............................................................................. 3
Network WaveLinx ................................................................................ 4
WaveLinx Device IP Address Assignment (DHCP or Manual) ................. 5
System Overview .................................................................................. 5
Product Overview .................................................................................. 5
System backbone IT information .......................................................... 6
Network Ports and Usage ..................................................................... 6
Network LAN and WAN ....................................................................... 6
VLAN .................................................................................................... 6
IPv6 readiness ....................................................................................... 6
Wireless Mesh Network Overview ....................................................... 6
Coexisting with Wi-Fi .......................................................................... 6
Channel Selection ................................................................................ 7
Low Airtime Consumption .................................................................. 7
Interference Tolerance ......................................................................... 8
Potential causes for signal disruption .................................................. 8
Administration and Maintenance ......................................................... 8
Configuration and Management tools ................................................. 8
Internal web pages .............................................................................. 8
Mobile application ............................................................................. 8
Certificates .......................................................................................... 9
User management, roles and access .................................................... 9
Backup and Restore ............................................................................ 9
Firmware and Software updates ......................................................... 9
Remote Support .................................................................................... 9
Firewalls (packet filtering, stateful inspection, proxy gateways) .......... 9
Redundancy and power failure ............................................................ 9
Third party integration ....................................................................... 10
Currently supported integration ......................................................... 10
API’s .................................................................................................. 10
Cloud connectivity .............................................................................. 10
Security ............................................................................................... 10
Physical security ................................................................................ 10
Customer security ............................................................................. 10
Device communication security ......................................................... 10
Network communication security ...................................................... 10
Network segmentation security .......................................................... 11
OTA update security .......................................................................... 11
COE assurance ................................................................................... 11
OSI model security ............................................................................ 11
Cybersecurity reporting and mitigation plans ..................................... 11
Cybersecurity or functionality issues and reporting ......................... 12
Eaton’s view on cyber security ........................................................... 12
Network and IT Considerations

WaveLinx Network Topology Options

WaveLinx is a wireless lighting control system that provides easy to install and implement energy code compliance, while providing a framework for future smart building requirements. The WaveLinx system uses IEEE 802.15.4 to communicate to the WaveLinx enabled smart devices from the centralized Wireless Area Controller (WAC-POE). Each wireless device then controls the connected driver, ballast, or control unit over a wired connection, limiting the traffic on the wireless network.

The wireless network is used to gather and transport energy and occupancy data to the Wireless Area Controller. The WAC-POE provides access to the WaveLinx wireless devices simplifying configuration and management of the lighting control system.

The WaveLinx wireless devices communicate using IEEE 802.15.4 wireless communication protocol that includes AES encryption for security.

The Wireless Area Controller (WAC-POE) is typically mounted centrally located above the ceiling in the space it is controlling. The Wireless Area Controller can provide a dedicated, not connected to building IT network or optionally can connected to the building IT network for additional features.

The section below explains the Dedicated and Network installation methods.

Dedicated WaveLinx

Stand alone space | IT setup not required | Scalable to join Network

- The Wireless Area Controller does not connect to the physical building IT network at all.
- The Wireless Area Controller provides a Wi-Fi access point for the WaveLinx mobile application connection using WPA2 wireless encryption and secure network username and password.
- The Wireless Area Controller still uses AES 128-bit encryption for all WaveLinx device to device network communications.
- Wi-Fi is used for communications from the phone smart device to the Wireless Area Controllers for programming, configuration and personal control through the use of the WaveLinx mobile application.
- The Wireless Area Controller provides a Wi-Fi access point with DHCP and uses HTTPS(TLS1.2) as part of its security access for the internal web pages and WaveLinx mobile application connections.
- The available Wi-Fi access point in the Wireless Area Controller is automatically disabled if it is connected to the building IT and receives an IP address from the DHCP server on the building network.
Network WaveLinx

Entire building solution | Smart building ready | Simple, secure network addition

- The Wireless Area Controller connects to the building IT network via PoE switch or power injector and must have access to the building DHCP server or configured to use a static IP via the WAC internal web pages.
- At the discretion of the building IT personnel the Wireless Area Controllers may be setup on a separate lighting network or VLAN.
- Wi-Fi is used for communications from the phone smart device to the Wireless Area Controllers for programming, configuration and personal control through the use of WaveLinx mobile application.
- The available Wi-Fi access point in the Wireless Area Controller is automatically disabled if it is connected to the building IT and receives an IP address from the DHCP server on the building network or if the WAC is configured to use a network routable static IP.
- Smart devices should be able to connect to the building Wi-Fi network and have access to the Wireless Area Controllers on the building IT network or VLAN.
- Connecting the Wireless Area Controllers to the building IT enables certain features such as BACnet® integration or future smart building integration features.
WaveLinx Device IP Address Assignment (DHCP or Manual)

Table 2: IP Address Assignments

<table>
<thead>
<tr>
<th>Device</th>
<th>Dynamic Addressing</th>
<th>Static Addressing</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAC (Wireless Area Controller)</td>
<td>Supported</td>
<td>Supported (default)</td>
<td>192.168.100.1 (default) • The WAC is the controller and gateway to the WaveLinx devices. • The WAC separates the IT and OT networks • The WAC is centrally located in the space above the ceiling (preferred) to wirelessly communicate to the OT WaveLinx devices via IEEE 802.15.4</td>
</tr>
<tr>
<td>Smart Device (phone or tablet)</td>
<td>Supported</td>
<td>Not Supported</td>
<td>• DHCP address provided by WAC when installed as a dedicated WaveLinx installation. • DHCP address provided by building IT wireless access point when installed as a network WaveLinx installation</td>
</tr>
</tbody>
</table>

System Overview

The Wireless Area Controller (WAC) is the main component of the Eaton WaveLinx Wireless Connected Lighting system. WaveLinx eliminates the cost and complexity of typical wireless control system commissioning while providing a wired, flexible, and reconfigurable wireless topology for on the fly space adjustments. The WaveLinx system meets modern code and utility requirements, delivers energy and cost savings, while enabling buildings to become smart buildings.

The WAC coordinates between the WaveLinx Mobile App and various WaveLinx devices to create communications and a building ecosystem that provides out of the box functionality and leverages our patent pending automatic code commissioning features. Using standards-based wireless mesh compliant topology the WAC communicates to various WaveLinx standards-based devices to provide area, lighting zone configuration, monitoring, and control.

The WAC provides centralized coordination of multiple areas for partial ON/partial OFF scheduling, demand response, lighting, occupancy, daylight settings and scene control. A single WAC can be connected to the building LAN to coordinate up to 16 areas, or multiple WAC’s can exist on a building LAN to scale the system to hundreds of areas all accessible for setup, configuration and control through the WaveLinx Mobile App.

Product Overview

- Wireless Area Controller (Gateway)
  - IEEE 802.11
  - IEEE 802.15.4
- WaveLinx Mobile App (Commissioning and user personal control)
  - IEEE 802.11
- WaveLinx Wallstation (Manual lighting and scene control)
  - IEEE 802.15.4
- Wireless Integrated Sensor (Fixture integrated occupancy sensor, ambient light sensor and control)
  - IEEE 802.15.4
- WaveLinx Tile-mount Sensor (Fixture with remote ambient light sensor and control)
  - IEEE 802.15.4
- WaveLinx Relay Switchpack with 0-10V (Relay zone control)
  - IEEE 802.15.4
- WaveLinx Receptacle (Wall mounted power outlet)
  - IEEE 802.15.4
- WaveLinx Room Based Sensor (Ceiling mounted PIR occupancy sensor)
  - IEEE 802.15.4
**System backbone IT information**

**Network Ports and Usage**

To ensure proper system operation the network ports and protocols listed below must be available to the WaveLinx Wireless Area Controller and the building IT infrastructure.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>WaveLinx Device</th>
<th>Usage</th>
<th>Description</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>80</td>
<td>WAC</td>
<td>Redirects to Configuration Webpages</td>
<td>Always Open</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>WAC</td>
<td>Configuration Webpages</td>
<td>Always Open</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>TCP</td>
<td>52725</td>
<td>WAC</td>
<td>SSL secured CAPI web services</td>
<td>Always Open</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>67</td>
<td>WAC</td>
<td>DHCP Server</td>
<td>Only open in Dedicated WaveLinx mode. Closed when connected to building IT</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>68</td>
<td>WAC</td>
<td>DHCP Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>546</td>
<td>WAC</td>
<td>DHCPv6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>547</td>
<td>WAC</td>
<td>DHCPv6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>5353</td>
<td>WAC</td>
<td>mDNS (Avahi)</td>
<td>Always Open</td>
<td></td>
</tr>
</tbody>
</table>

The following ports are closed by default.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>WaveLinx Device</th>
<th>Usage</th>
<th>Description</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22</td>
<td>WAC</td>
<td>SSH</td>
<td>Closed by default. Admin may open via webpages</td>
<td>TLS 1.2</td>
</tr>
</tbody>
</table>

**Network LAN and WAN**

WaveLinx was designed so that no WaveLinx devices with the exception of the Wireless Area Controller interface directly with the LAN or WAN within the building. All WaveLinx devices must communicate to the Wireless Area Controller to maintain proper network separation and security.

**VLAN**

Multiple WaveLinx Wireless Area Controllers can be installed on a VLAN within the building IT network using Layer 2 or Layer 3 network switches. When implementing a VLAN you must ensure the mobile devices used to configure and manage the WaveLinx system also have access to that VLAN.

VLAN's are not required for the WaveLinx system to work, however they can be implemented on sites that have the IT support and require separation of networks for additional security.

**IPv6 readiness**

WaveLinx hardware is designed to be IPv6 capable including end devices, currently using IEEE 802.15.4 MACPHY, which use silicon from suppliers that specify that their solutions are Thread and IPv6 capable.

**Wireless Mesh Network Overview**

WaveLinx Wireless Connected Lighting uses a low duty cycle, narrow-band, IEEE 802.15.4 ZigBee® HA1.2-based 2.4 GHz wireless protocol that is not known to interfere with 2.4 GHz Wi-Fi or other systems. Each WaveLinx Wireless Area Controller and associated mesh network (typically up to 200 wireless devices) can also be configured via internal web pages to use a specific IEEE 802.15.4 channel to avoid co-channel interference with other installed 2.4 GHz equipment. IEEE 802.15.4 channels 11-24, corresponding with 5 MHz-wide frequency bands from 2.405 GHz to 2.480 GHz may be assigned to specific wireless mesh networks. The wireless communication is secured and encrypted using AES 128-bit encryption.

**Other Notes:**

- **Radio**: 2.4GHz
- **Standard**: IEEE 802.15.4
- **Transmitter Power**: +7dBm
- **Range**: 50m (150ft) LOS
- **# of Walls**: 2 interior walls standard construction

**Coexisting with Wi-Fi**

The WaveLinx Wireless Connected Lighting system employs three techniques to either eliminate or drastically reduce its impact on Wi-Fi networks in the building:

- **Channel Selection**: This technique involves identifying WaveLinx IEEE 802.15.4 communication channels that do not overlap with the current Wi-Fi deployment.
- **Low Airtime Consumption**: WaveLinx is designed to reduce wireless communications during steady state operation, greatly reducing the
probability of collision with Wi-Fi traffic.

- **Interference Tolerance**: WaveLinx is designed to work reliably despite encountering some interference, by detecting if communications packets are lost and retransmitting if needed.

### Channel Selection

WaveLinx uses IEEE 802.15.4 channels, which are within the same 2.4 GHz frequency band that IEEE 802.11 Wi-Fi operates within. Since devices communicating on the same channel can cause interference, the devices need to be set on channels that do not overlap.

If we overlay the most frequently used channels used by IEEE 802.15.4 (WaveLinx) and IEEE 802.11 (Wi-Fi) on the chart below, you can see there is no overlap.

Wi-Fi uses channels 1, 6 and 11 by default, and IEEE 802.15.4 devices should be set to use channels 14, 15, 19, 20, 24, 25, and 26 by default which fall within the gaps of the Wi-Fi channels. For IEEE 802.15.4 channels 15 and 20 are typical and allow us to prevent overlap that can lead to potential signal interference. Channels 25 and 26 are typically not used in North America because they are too close to a restricted RF band.

Ultimately this means that IEEE 802.11 Wi-Fi and IEEE 802.15.4 wireless devices can co-exist in the same space without interference if they are properly set with the correct channels.

### Low Airtime Consumption

WaveLinx recognizes that it is not always possible to select non-overlapping channels. Many Wi-Fi access points aggressively use all available spectrum to maximize performance. To coexist with such solutions, WaveLinx is designed to send two messages every five minutes per sensor. The following example shows the airtime consumption for a 50,000 square foot installation.

- Airtime Consumption = \# sensors * msgs_per_sensor * airtime_per_msg / 5mins * 100%

- 50,000 square feet = 500 sensors

- 1.5 ms of airtime per message

- Airtime Consumption = 500 * 2 * 1.5ms / 5mins * 100%

- Typical Airtime Consumption = 0.5%

With such low airtime consumption, the WaveLinx system will easily coexist with Wi-Fi networks whether or not non-overlapping channels are used.

### Interference Tolerance

In addition to ensuring that there is no impact on Wi-Fi installations, the WaveLinx Wireless Connected Lighting system must be tolerant of interference by other Wi-Fi and IEEE 802.15.4 networks. The selection of non-overlapping channels serves to avoid the potential problem.
In addition, WaveLinx is designed to be loss tolerant. The WaveLinx communications increase transmission reliability through the use of acknowledgments and packet retransmission. As a result, when a packet is lost, the loss is detected and corrected through retransmission. Additionally, WaveLinx is designed to perform lighting control without requiring network communication at all. Lighting control will continue to operate in the event of a complete wireless failure.

Potential causes for signal disruption
As stated above WaveLinx should be able to co-exist in the building with Wi-Fi installations, however there are many causes of interference and degradation that go beyond the scope of this document. Some basic things that can be addressed during the design phase that may aid in preventing issues include.

1. Review the network range and the distance between the devices. It is just a fact of how signals work that the further the distance between devices, the lower the signal strength. Both IEEE 802.15.4 wireless and IEEE 802.11 Wi-Fi have a maximum unobstructed “line of site” point to point range of 100 meters. However, we also need to factor in obstacles which are prevalent in our indoor spaces.
   a. Of special consideration are the quantity and materials and thickness of walls and other obstacles that are between transmitting and receiving devices. Wireless signals can have trouble communicating through these solid objects reducing the wireless range.
   b. Transmitter and end device placement planning during the design phase is critical to ensure proper coverage range and proper device functionality. Manufacturers may have specific recommendations for ranges for their devices that are important to pay attention to.

2. Review the location of the transmitters. Placing two transmitters within the same space, even if they are on different frequencies and channels can lead to disruption if they are too close together.
   a. If too close together, they may increase their signal to “shout” over the other transmitters in the space. If both transmitters are shouting, devices cannot hear or respond. Commercially available wireless products often state in their instructions to maintain at least a 5 to 10 foot air gap between other wireless transmitters to prevent this type of interference by proximity.

3. The quantity of devices on the network can also be a factor of signal degradation. Different network types may support different quantities of nodes. In addition, depending on the design, the quantity of devices may slow or degrade the signal. It is important to review recommendations of device limitations described by the wireless system manufacturers and incorporate this into the design.

Administration and Maintenance

Configuration and Management tools
WaveLinx uses internal webpages within each WAC to manage that section of the WaveLinx system. The internal webpages are accessed by connecting to the WAC IP address via your browser and allow for network configuration.

The WaveLinx mobile application is used for configuration of your lighting control areas and functionality. The WaveLinx mobile application connects either directly to each WAC or to the building IT wireless network to access all WAC’s connected to the building network.

Internal web pages
- The WaveLinx internal web pages permit the following configuration and management settings:
  - Time synchronization
  - User management
    - Administrator - user name and password
    - User – username and password
  - Certificate management
  - Backup/Restore
  - Network management
    - DHCP/Static
    - WLAN access
      - SSID
      - Password
  - Firmware update of WAC and all connected devices
  - EULA

Mobile application
- The WaveLinx mobile application permits the following configuration settings:
  - Define Areas
  - Create/modify Zones
  - Identify/modify/add devices
  - Create/modify occupancy sets
• Create/modify daylight sets
• Create/modify schedules
• Modify demand response
• Modify wallstation button programming

Certificates
WaveLinx uses Eaton provided SSL Certificates by default that are installed with the system and ensure the mobile device and Wireless Area Controller communications.

At the building IT departments discretion custom certificates can be created and installed on the mobile device and Wireless Area Controller to provide additional security.

User management, roles and access
User authentication is required for administration and user access to each WaveLinx Wireless Area Controller. The WaveLinx system currently supports three levels of user access.

• Administrator
• User
• 3rd Party Interface

WaveLinx does not currently support single sign on or LDAP access through the building network.

Backup and Restore
WaveLinx supports backup and restore process through internal webpages of the Wireless Area Controller(WAC). Each WAC performs its own backup of all programming and network information, that can be restored in the event of a product failure and it needs to be replaced.

Backups should be done periodically to ensure you have the latest backup. It is recommended that you perform a temporary backup of data prior to doing a firmware update to the system, in the event something should be updated incorrectly. Once the firmware update has completed successfully a permanent backup can be done, and stored per standard building IT processes.

Firmware and Software updates
WaveLinx Wireless Connected Lighting supports firmware updates to all WaveLinx wireless devices. These updates include a digital signature to ensure they are valid prior to being installed on the wireless devices.

Firmware updates are uploaded to each Wireless Area Controller which manages the distribution and installations to all WaveLinx devices.

Mobile application updates are handled through software updates through Android and iOS stores.

Firmware and software updates are typically released on a semi-annual basis for normal activities. Major improvements and feature enhancements are scheduled for a yearly release.

If your WaveLinx system is registered with Eaton Lighting Solutions the registered user will get an automatic notification of firmware and software updates. Additional information will be provided through website information.

Remote support
For some configuration and diagnostics purposes our technical services staff may offer remote access services. This may be accomplished in several ways depending on the customer’s network configuration and IT requirements. Most often temporary access is provided by the customer’s network system administrator and any required 4G modem installation, VPN access, port opening and/or credentials are revoked upon completion of the required support service.

Special service programs could be arranged through the Eaton Service and Support Group.

Eaton’s Lighting Division has a dedicated team within the Eaton Service and Support Group.

This support team is required to go through standard ethics, Global Internet security and other courses yearly and are subject to a background check as part of Eaton employment.

Firewalls (packet filtering, stateful inspection, proxy gateways)
These items should be handled as needed by the local building IT department. The implementation of these security features would be the responsibility of the IT network architect and would not interfere with the standard operation of the lighting system as that is occurring on the OT network.

Additionally the WaveLinx Wireless Area Controller/Gateway includes a firewall isolating the IEEE 802.15.4 based lighting device and sensor network communications from the IEEE 802.3/IEEE 802.11 based LAN/WAN network.

Redundancy and power failure
The WaveLinx system allows for complete system backup capabilities. Redundant PoE power to the WaveLinx Wireless Area Controller is
the responsibility of the building IT department.

In the event of loss of communications with the WaveLinx Wireless Area Controller due to communications failure or power failure the WaveLinx devices will continue to maintain their current light level for at least 1 hr. After 1 hour of lack of communications the WaveLinx devices will continue to operate in out of the box mode with individual luminaire occupancy being the primary method of control.

The WaveLinx system is designed to be able to be compliant with UL924 emergency lighting standards as long as the appropriate devices are included in the system design.

**Third party integration**

The WaveLinx Wireless Area Controller (WAC) can interface with other systems via IP connection. In the future WaveLinx will allow further integration through enterprise-level software and server called Lighting Xpert InSights.

**Currently supported integration**

Demand Response is currently supported through an IP connection into each WAC from the building management system or other third party system. See the WaveLinx Demand Response application note for more information on the connection.

**API’s**

WaveLinx supports an API for integration however it does not provide the ability to change software programming of the system. API’s are used for status and override of current state.

**Cloud connectivity**

WaveLinx does not require cloud connectivity to support any lighting control functionality. The system was designed to be supported completely on premises.

In the future cloud connectivity will be supported for value added applications and data storage and remote updates. The lighting control functionality will always be maintained on premises.

**Security**

Eaton views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the WaveLinx Wireless Connected Lighting (WCL) System employs current industry best practices to reduce, identify, contain and manage security risks. WaveLinx has been designed and engineered with wireless security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. The Eaton Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the development of WaveLinx and offers Eaton customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain Eaton product solutions in a secure environment. More information on the Eaton PCCoE can be found at www.eaton.com/cybersecurity

The WaveLinx System uses a multi-tiered approach to addressing industry best practices for security risk management and utilizes guidelines promulgated by the Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST) and industry standards organizations to achieve a secure and adaptable lighting control platform.

**Physical security**

- An architecture that isolates the wired Ethernet network from the wireless network, which strictly limits the possibility of the WaveLinx wireless being used as an access point to the corporate network and gain confidential information.

- Physical access also involves the customer location. This includes not allowing unauthorized personnel in areas where they do not belong, or access to devices they should not be connecting to.

**Customer security**

- Customer security process is a partnership between Eaton and the customer and involves multiple levels of password and network access protection.

- Beyond physical access the customer provides an additional layer of security with strong authentication to access their corporate wired or wireless network and limiting the devices that can access those networks.

- Eaton provides additional protection with unique username and password requirements for each Wireless Area Controller that are securely stored per NIST-recommended best practices.

**Device communication security**

- For secure device-to-device communications, encryption is an important factor to reduce the potential of someone reading data sent on the network. For that reason, all WaveLinx communications use AES 128-bit encryption, recommended by NIST as part of FIPS publication 197.

**Network communication security**

- WaveLinx uses secure HTTPS (TLS1.2) protocols for securing connections to the Wireless Area Controller over the wired network.

- WaveLinx uses secure WPA2 Enterprise technology for secure connections to the Wireless Area Controller over the Wi-Fi network when acting as an access point. If the Wireless Area Controller is connected to a wired network for communications this connection method is disabled.

- WaveLinx mobile applications uses HTTPS (TLS1.2) as part of its communications to the Wireless Area Controller regardless of connection
method, which means only our mobile application can send data to the WaveLinx system

Network segmentation security
- Each Wireless Area Controller employs its own unique keys, which limits any potential breach to only a small area of the system.
- The WaveLinx Wireless Area Controller (WAC) provides segmentation between the lighting Operational Technology (OT) network and the enterprise Information Technology (IT) network.
- The IT/OT network segmentation provides a barrier to possible IT network attack surface exposure. Even if an attack within the lighting (OT) network and its devices is successful, the WAC isolates the enterprise IT network from potential attack.

OTA update security
- WaveLinx provides a method to allow for digitally signed firmware update files to be sent to the devices over the air (OTA). It is imperative as part of network security to ensure OTA updates are digitally signed firmware images from their manufacturer so the devices recognize they are valid updates from that manufacturer and not sent with a malicious intent.

COE assurance
- Eaton's Product Cybersecurity Center of Excellence involvement and guidance was key as part of the WaveLinx development to ensure our product incorporates industry and governmental network security best practices.
- The PCCOE also provides a publicly accessible site for information and feedback concerning cybersecurity threats and responses, as well as a method for you to monitor network breach risks.

OSI model security
WaveLinx supports a seven layer multi-tiered approach to security, below we illustrate how WaveLinx supports security through the entire seven layer OSI model, not just the WaveLinx application.

Cybersecurity reporting and mitigation plans
Eaton’s Product Cybersecurity Center of Excellence (PCCOE) involvement and guidance is key as part of all current and future development to ensure our product incorporate industry and governmental network security best practices.

Eaton considers latest available best industry practices (DHS, NIST, FIPS) to reduce, identify, contain and manage risks: Deter, Protect, Detect, React, Recover

The PCCOE also provides a publicly accessible site for information and feedback concerning cybersecurity threats and responses, as well as a method for you to monitor network breach risks.

See www.eaton.com/cybersecurity for more detail.
Cybersecurity or functionality issues and reporting

Issues found in the field can be reported to Eaton service and support group, who will attempt to replicate the issue. If the issue can be replicated it is reported through internal issue tracking software which assigns the issue to the engineering team for resolution.

Depending on the severity and priority of the reported issue, this could include standard firmware or software updates published to the website or a proactive service visit by Eaton service and support group.

Eaton’s view on cyber security

Eaton views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the all Eaton connected lighting systems employ current industry best practices to reduce, identify, contain and manage security risks. These systems have been designed and engineered with wireless security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. The Eaton Product Cybersecurity Center of Excellence (PCCoE) provided guidance throughout the development of each system and offers Eaton customers an Internet accessible portal to identify emerging threats, find ways to secure products against them and help customers deploy and maintain Eaton product solutions in a secure environment. More information on the Eaton PCCoE can be found at www.eaton.com/cybersecurity.