PHILIPS

dynalite

Controls

Security Statement

Contents

1 Introduction 3

2 System Architecture and Security 4
RS-485 connections 5
Ethernet connections 6
2.1 Integration with other systems 10

3 Network Security 11
3.1 Enterprise clients 11
3.2 Ethernet devices 11
3.3 API & websocket 11
3.4 Integrated systems 12

4 Device and Physical Security 13
4.1 Firmware updates 15
4.2 Decommissioning 16
4.3 Product replacement 17

5 Cloud services 18
5.1 Encryption and key management 18
5.2 Business continuity 19
5.3 Authentication and authorization 19
5.4 System updates 19

6 Data Classification and Inventory 20

7 Compliance to (International) Standards 21

8 Shared Responsibility Model 21
8.1 Responsibilities 21

9 Secure Installation Requirements (for customers) 24
9.1 Additional hardening requirements 26
9.2 Security Configuration options 27
9.3 Instruction and Recommendation for Security Tooling 28
9.4 Security Maintenance Activities 28
9.5 Security Mitigation 28

10 Security Operations Requirements (for Customers) 29
10.1 Accounts on server and devices 29

11 Security Maintenance Requirements (for Customers) 30

12 Security Incidents 31
12.1 How to report a Security Incident 31

13 Coordinated Vulnerability Disclosure 31
13.1 How to report a vulnerability 31

14 Known Vulnerabilities and Security Advisory 31

15 Legal Disclaimer 32

1 Introduction

Philips Dynalite manufactures a portfolio of controls products designed for connected lighting systems. Systems are implemented with a combination of hardware, software, protocols, integrations, and services that together provide a complete solution for smart buildings.

As connected lighting systems are an integral part of the Internet-of-Things (IoT), they also have similar security risks as other internet-connected devices.

Most companies use well-established procedures to reduce the risk of data breaches on devices connected to their IT networks. Company-issued computers, smartphones, tablets, and so on are considered attack vectors and must comply with certain rules to be trusted and granted access to internal corporate networks. The same procedures apply to IoT systems connected to a customer's network.

The key concerns regarding IoT solutions deployed on a network are:

1. Vulnerabilities that result in access to devices or network components on the corporate IT network.
2. Vulnerabilities that disturb operational performance of individuals or equipment working in a building.
3. Vulnerabilities in IoT devices that can be exploited to compromise other services.

This document addresses the Philips Dynalite IoT security aspects by providing:

- A description of the security architecture and implemented security features. The measures (technical and procedural) that we (Signify) have implemented. This includes a description of secure connections between the System Manager (SM) Server, Ethernet gateways and control devices, as well as user access to the server, SM Configurator, SM client software and API-based interfaces.
- An explicit list of all security items that that we consider the responsibility of the customer, including system hardening to minimize potential residual security risks on the SM server and integrated third-party systems.
- Information and useful links to report security incidents and vulnerabilities.

This document is in addition to the general Signify security policies and procedures. It details the security initiatives Signify has taken to develop and deploy Philips Dynalite systems and the measures to be adopted by customers for secure installation, operation, maintenance, and decommissioning.

See the General Product Security Statement for more information
https://www.signify.com/global/product-security/professional-systems-and-services

2 System Architecture and Security

The Philips Dynalite product portfolio has many inbuilt features with a wide range of applications providing a scalable IoT solution. Our devices may be networked over Ethernet or RS-485 and communicate with each other via the DyNet protocol. Systems are often custom designed to fit the needs of each project.

Software applications are available for users to design, build, configure, control, monitor and manage their lighting control system with customizable templates to help fast-track common system settings. In addition, the software can provide users with an interactive visual representation of their system, automated and manual controls, alert notifications, API access and analytics for an entire floor, building or group of buildings.

Although products include a variety of security measures, they have the following characteristics in common:

- Products are connected to a network and contain (configurable) software/firmware.
- Products have software/firmware update capability over the network.
- Products can be accessed and/or operated remotely via common networks.

The Philips Dynalite portfolio consists of the following products:

Hardware

- User interfaces
- Multifunction sensors - Light intensity and motion detection
- Network devices
- Electrical accessories
- Load controllers (Switching, Signal dimming, Power dimming, Multipurpose, HVAC)
- Integration gateways

Software

- System Builder - design and commissioning software
- System Manager software suite - Configuration Tool, SM Client, Desktop Switch App, System Dashboard, and API for third-party interfaces
- Mobile control apps

Philips Dynalite products are designed as on-premises systems based on our modular controls architecture. Devices are typically connected in a trunk-and-spur topology. System Manager head-end software and gateways are connected to the (Ethernet or RS-485) trunk network. Gateways then connect to RS-485 spur devices on each floor. Gateways manage traffic from the spur networks to the trunk network. In addition, specific hardware and software gateways enable integration with other building systems.

Spur devices such as load controllers, user interfaces, sensors and integration devices form a field network that is installed throughout the building. Devices communicate with each other using the DyNet protocol and operate independently of the System Manager head-end software.

Load controllers have flexible outputs to control lighting, power sockets, air conditioning, window coverings, fans etc. Signal controllers can also have protocol-based outputs such as DMX, 1-10V, DSI, DALI Broadcast, DALI Enumerated. DALI-2 driver controllers can also host sensors and dry contact interfaces on the DALI bus.

Firmware, software, and configuration updates are deployable over the network to ensure devices are running the latest versions.

Devices fit into one or more of two security categories based on their available physical connections:

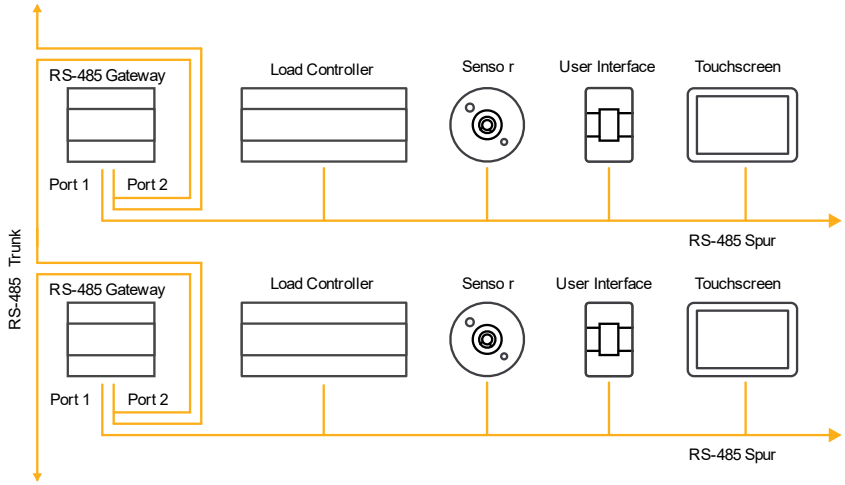
1. RS-485 connections
2. Ethernet connections

RS-485 connections

Most Dynalite devices have an RS-485 port to connect to the spur field network on each floor. Gateways then connect the spur networks to the trunk network in the building. Trunk networks can be Ethernet or RS-485.

The RS-485 network is dedicated exclusively to the lighting control system and access to the network is only via direct physical connection or via a gateway/bridge. DyNet over RS-485 is not a secure protocol, so devices with RS-485 ports must be physically secured by installation in a secure enclosure/room, with wiring kept physically inaccessible to unauthorized persons.

Where Ethernet gateways/bridges integrate with the RS-485 field network, they use authentication and network firewalls to ensure secure access so only allowed messages are passed to the RS-485 field network. Gateways can be reconfigured, and factory-reset from the RS-485 network.



D Dynalite controllers may have DMX512 outputs and/or DALI outputs for connecting to lamp drivers and input devices. DMX bus and DALI bus security risks are not covered in this document as they are lighting control industry standards.

Ethernet connections

Ethernet/optical fiber is often used for the IP trunk network. An Ethernet spur may also be connected to other Ethernet devices, such as the PDZG-E wireless gateway. Ethernet connection security depends on each device's capabilities. There are currently five Ethernet enabled devices in the product portfolio that provide gateway/bridging functionality to other parts of the system.

Ethernet Gateways

- PDDEG-S
- PDEB/PDEG
- PDZG-E

Ethernet enabled load controllers

- DDRC-GRMS-E
- DDBC320-DALI

PDDEG-S

The PDDEG-S can be used for multiple functions in the system. The three most common functions are:

- Cloud Gateway – providing a secure internet connection to the building.

  The PDDEG-S connects securely over the internet to the Dynalite cloud, and via Ethernet or RS-485 to the on-site Dynalite control network. The client or integrator may choose to connect their network to services running in the cloud and have the collected data stored remotely in the cloud. The PDDEG-S manages and secures the traffic from the on-premise system to the cloud.

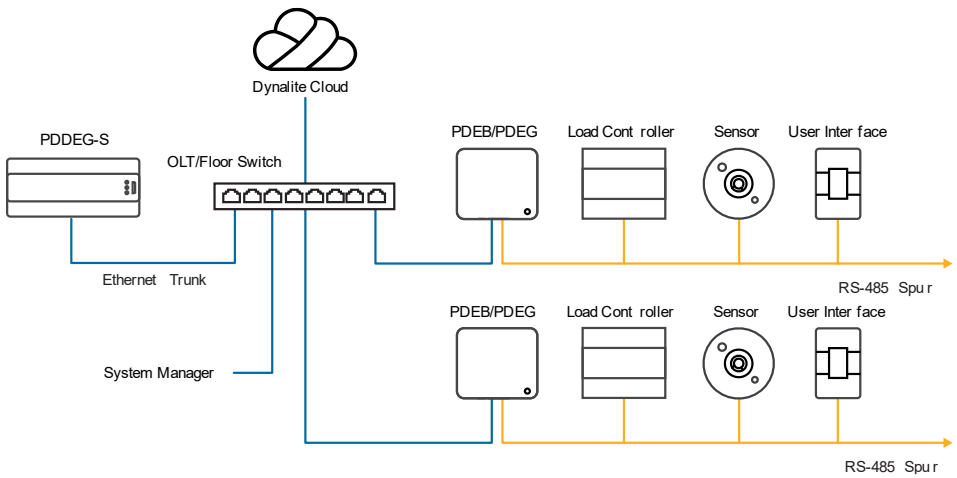
  Internet access to a PDDEG-S is secured with Transport Layer Security (TLS) and accessed remotely with an encrypted, authenticated connection via the Dynalite Cloud Platform. To enable remote access, the user must:

  a. Set up an online Interact Account
  b. Login to their Interact Account from System Builder
  c. Configure the cloud gateway
  d. Upload a site certificate to the gateway
  e. Register the cloud gateway in the Dynalite Cloud Platform
  f. Save the job to the cloud

  Network traffic between SM and a PDDEG-S may be secured with a TCP TLS connection by uploading a Site Certificate to both the SM server and to the PDDEG-S. The architecture uses a client/server relationship from the System Manager to the PDDEG-S, ensuring that intruders on the IP lighting control network cannot initiate a connection to SM.

  Network traffic to a PDEB/PDEG is unsecured. The routing configuration in each gateway/bridge prevents intruders from controlling or intercepting traffic between spurs.

  Access to the inbuilt webserver can be authenticated with a username and password and secured via HTTPS by uploading a Web Server Certificate.



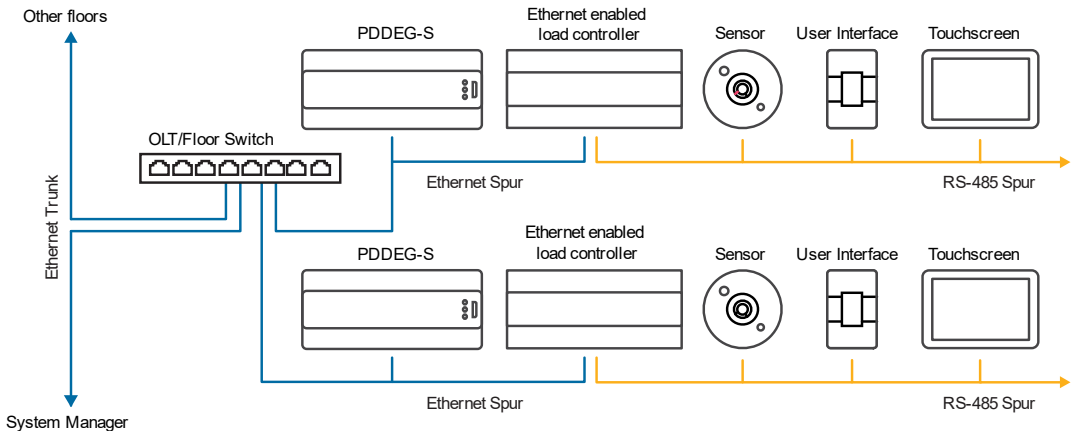
- Ethernet Gateway – providing a network bridge between the Ethernet trunk and an Ethernet or RS-485 DyNet spur.

  Network traffic between SM and the PDDEG-S is secured with a TCP TLS connection by uploading a Site Certificate.

  Network traffic between PDDEG-S and an Ethernet enabled load controller is secured using a TCP TLS connection by uploading a Site Certificate. The architecture uses a client/server relationship from the Ethernet enabled load controller to the PDDEG-S. This ensures that intruders on the IP network cannot initiate a connection to an Ethernet enabled load controller.

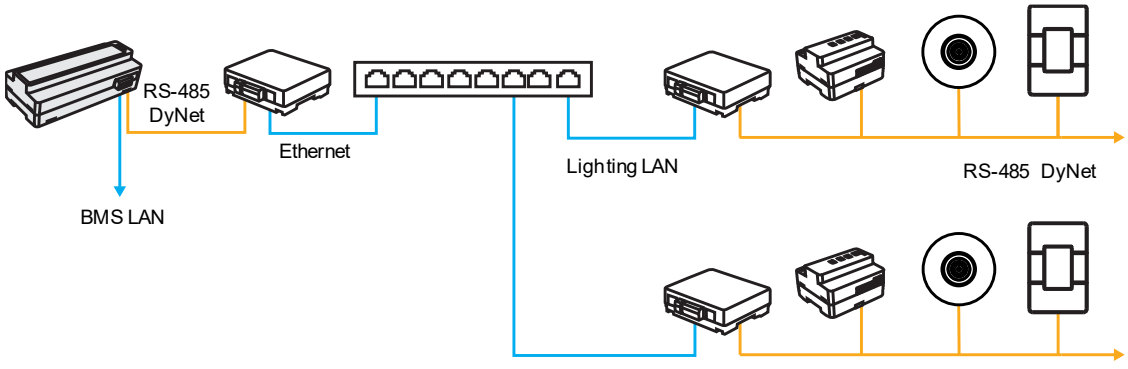
  Other devices may be connected to the PDDEG-S RS-485 port, with the required physical network security measures in place. For more details, refer to the Ethernet Gateways Commissioning Guide and Interact Hospitality Commissioning Guide.

  Access to the inbuilt webserver can be authenticated with a username and password and secured via HTTPS by uploading a Web Server Certificate.



- BACnet gateway – providing integration between BACnet protocol (BMS) and DyNet protocol.

  BACnet is not a secure protocol. So, for security reasons we recommend keeping the two networks separate. It is possible to connect the BMS and lighting system on the same network, if required, however, this is not recommended, and the customer/installer is responsible for any security impact.

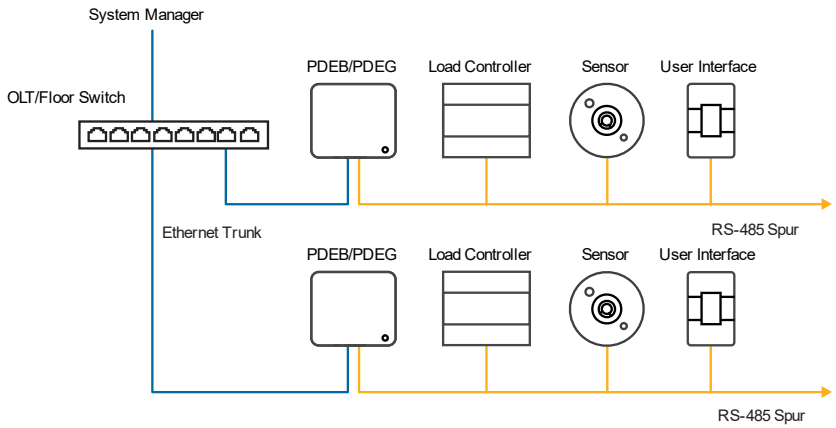


PDEB/PDEG

Network traffic between System Manager and the PDEB or PDEG is not secure and (where required by the customer) it may need to be implemented with physical and other appropriate network security measures. The routing configuration in each gateway/bridge prevents intruders from controlling or intercepting traffic between spurs.

Access to the inbuilt webserver can be authenticated with a username and password and secured via HTTPS by uploading a Web Server Certificate. There is no webserver on the PDEB.

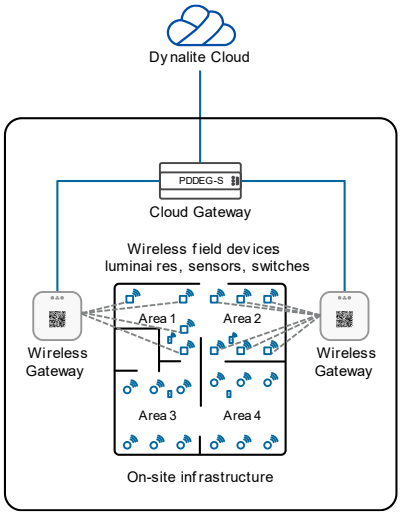
For more details on gateway architecture, refer to the Ethernet Gateways Commissioning Guide.



D The Philips Dynalite Touchscreen (PDTS) has an Ethernet port, that is used for configuration and maintenance purposes only. To maintain security in operation, the Ethernet port on the PDTS shall be physically disconnected and secured following service/maintenance procedure completion. For more information refer to the PDTS Commissioning Guide.

PDZG-E

The PDZG-E wireless gateway integrates a wired IP lighting control network with a Signify wireless lighting control network. Network traffic between the PDDEG-S Ethernet gateway and the PDZG-E wireless gateway is secured using a TCP TLS connection to prevent interception or unwanted injection of messages.



The overview diagram details a simplified architectural view of PDZG-E connections. Lighting control is implemented using a Zigbee wireless mesh network. The system is built using a PDZG-E wireless gateway and multiple lighting devices that are registered in the project file stored in the cloud. The PDZG-E has an Ethernet interface to securely connect to the IP network and a wireless transceiver that communicates with wireless lighting devices. Each wireless lighting device has a wireless transceiver that communicates with other devices in that network.

Wireless lighting devices and luminaires communicate using a Zigbee network, which uses AES encryption with a 128-bit key for protection. AES is a symmetric key encryption scheme, which relies on a 128-bit shared secret key used for encryption and decryption of network data.

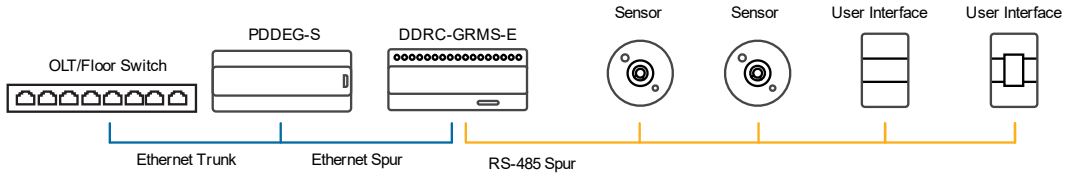
Large systems are designed by creating multiple wireless networks that each connect to a PDZG-E, which then connect to the lighting IP network. The network may also be connected to services running in the Dynalite cloud with data collected, stored remotely in the cloud.

DDRC-GRMS-E

Network traffic between the PDDEG-S Ethernet gateway and the DDRC-GRMS-E load controller is secured using a TCP TLS connection to prevent interception or unwanted injection of messages.

The architecture uses a client/server relationship from the DDRC-GRMS-E to the floor Ethernet gateway, ensuring that intruders on the IP network cannot initiate a connection to the DDRC-GRMS-E, in an attempt to control the RS-485 network. In addition, an IP connection is blocked to any user without a matching encryption certificate. This prevents any attempted malicious reconfiguration or reset commands from the IP network to the local devices.

Sitting between the DDRC-GRMS-E's Ethernet and RS-485 network ports, the DDRC-GRMS-E firewall blocks any attempt to pass unauthorized commands out to the spur network. Combining network encryption and firewalls provides comprehensive protection against system intrusion from the IP network to the RS-485 DyNet field network. The DDRC-GRMS-E does not have any user accounts.



For more details on DDRC-GRMS-E architecture, refer to the Interact Hospitality Commissioning Guide.

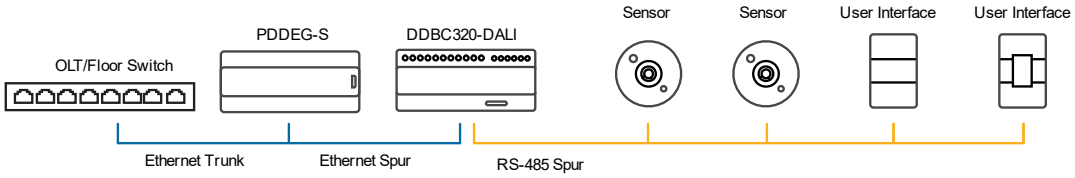
DDBC320-DALI

Network traffic between the PDDEG-S Ethernet gateway and the DDBC320-DALI load controller may be secured using a TCP TLS connection to prevent interception or unwanted injection of messages.

The architecture uses a client/server relationship from the DDBC320-DALI to the floor Ethernet gateway, ensuring that intruders on the IP network cannot initiate a connection to the DDBC320-DALI, in an attempt to control the RS-485 network. In addition, an IP connection is blocked to any user without a matching encryption certificate. This prevents any attempted malicious reconfiguration or reset commands from the IP network to the local devices.

Sitting between the DDBC320-DALI's Ethernet and RS-485 network ports, the DDBC320-DALI firewall blocks any attempt to pass unauthorized commands out to the network. Combining network encryption and firewalls provides comprehensive protection against system intrusion from the IP network to the RS-485 DyNet field network.

The DDBC320-DALI does not have any user accounts.



2.1 Integration with other systems

Hardware and software gateways support a choice of standard industry protocols and integration options.

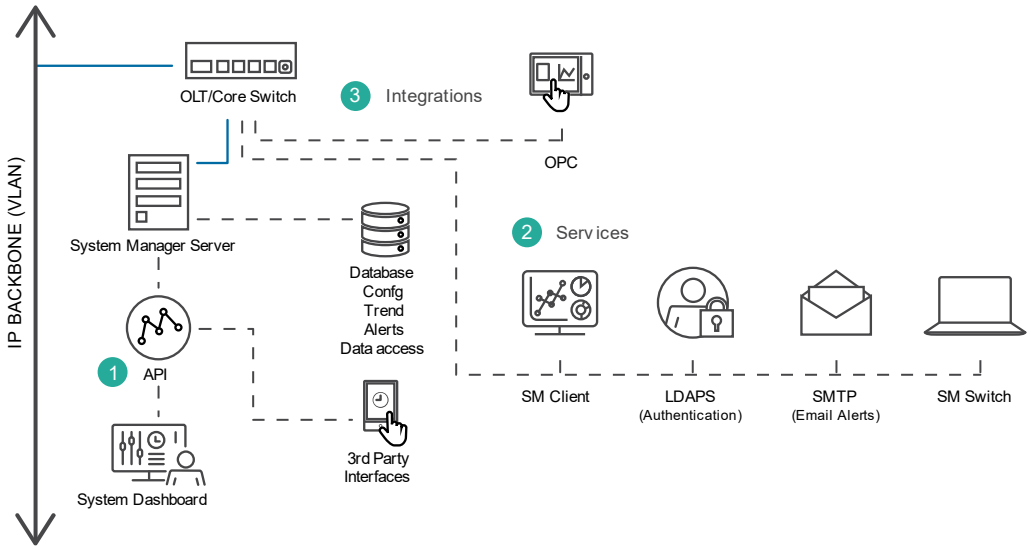
Integrations

- Software gateway integrations using System Manager with standard industry and proprietary interfaces and protocols, such as APIs, LDAPS, SMTP, OPC UA.
- Hardware device-based integration such as, 1-10V, DSI, DALI, DMX, KNX, LON, Somfy, Modbus, BACnet, Philips Hue, Infrared (RC5), RS-232, USB, TCP, UDP, FTP, Telnet, WebPage.cgi, Text over IP, API.

3 Network Security

System Manager Connections

In addition to being connected to the control system network, System Manager is also connected to the corporate IT network enabling access from enterprise clients and specific system integrations or API based integrations.



3.1 Enterprise clients

TCP/IP-connected client interfaces can be secured with encryption and authentication.

- System Manager clients – Enterprise client app with Windows users and Windows password policy.
- Windows user – Windows users and password policy may be configured centrally in Active Directory.
- SMTP server – email notifications.
- System Manager Switch – desktop lighting control app.

3.2 Ethernet devices

TCP/IP-connected devices are secured with TLS, initially via a default factory certificate, which is replaced in each device during commissioning with a unique site certificate.

3.3 API & websocket

The System Manager Server manages the system databases, enterprise clients and APIs to enable secure access from third-party interfaces.

The System Dashboard and third-party interfaces connect via the API/websocket.

- APIs use Windows Authentication by default. The server validates the username/password in the request against configured Windows users.
- The Dashboard has no authentication by default, but it can be configured as described in the Lighting API Online User Guide.
- Websocket events (sent from the server only) have no authentication.

For easy and secure login and password management, Windows users and password policy may be configured centrally in Active Directory.

3.4 Integrated systems

System integration facilitates communication for unified, sitewide intelligence with third-party network systems to exchange commands and data about system operation. Other systems can be integrated using a specific controller, gateway device or System Manager server. Both hardware and software gateways are highly flexible and are based on industry communication standards enabling a wide array of interconnectivity.

Connectivity to other systems is via industry protocols, that may not provide secure alternatives. Therefore, alternative mitigating security measures should be implemented. Integrations include:

Software Gateways	Hardware Gateways	Controllers
OPC UA (secure option)	Signify Zigbee wireless	0/1-10 V
OPC DA/AE	Philips Hue	DALI & DSI
SMTP (sending only)	BACnet	DMX512
	DMX512	Dry contact interface
	KNX	
	Somfy	
	Modbus	
	CoolMasterNet	
	RS-232	
	Analogue inputs	
	Dry contact interface	
	TCP, UDP, FTP, Telnet, Text over IP, CGI, API (secure option for TCP, UDP, CGI & API)	

4 Device and Physical Security

This section describes additional measures to protect the system by prohibiting physical access to the optional System Manager server, Ethernet gateway devices and RS-485 field network devices.

System Manager Server

It is advised that the System Manager Server is placed in a secure IT room to which physical access is monitored and restricted only to authorized individuals. It is also recommended to install all active servers and databases on the same machine.

Ethernet Gateways

Ethernet Gateways must be physically secured to prevent security breaches. They must be placed in a secure IT/utility cabinet to limit physical access only to authorized individuals.

Ethernet Gateways provide a connection between the field network and the trunk network. They authenticate with SM server when they become operational with unique secure user credentials.

Ethernet Gateways feature the following security measures:

- Webserver access via HTTPS
- Minimization of externally available services
- Only signed secure firmware updates are deployed
- Secure bootloader

Additionally, the PDDEG-S features the following security measures:

- Default secure port numbers
- Encrypted IP communications

The QR code on the PDDEG-S Ethernet Gateway allows easy identification of the device and contains the following information:

- Hardware version of the device
- Product name
- MAC address
- Serial number
- 12NC
- Default user password (default password must be changed upon installation)

Wireless devices

The PDZG-E wireless gateway is a wireless communication device that connects multiple Zigbee nodes, such as sensors, drivers, and so on. The wireless gateway translates between Ethernet and the Zigbee wireless network.

To create a system, an Ethernet Gateway and one or more PDZG-E's should be connected to a separate Ethernet network or VLAN without internet connectivity or connection to any other Ethernet networks in the building. It is recommended that physical access to the cabling is restricted to authorized individuals to isolate and mitigate any external security risks. Ethernet Gateways needs to be placed in a secure IT/utility cabinet to prevent unauthorized tampering.

Furthermore, it is recommended to restrict physical access to the PDZG-E devices by placing them against the ceiling or as high as possible on the wall, while remaining accessible for commissioning and maintenance purposes. It is important to ensure that wireless signal propagation is not compromised by maintaining line-of-sight to other wireless devices in the network.

The device features the following security measures:

- No hardware debug interfaces available
- Hardened operating system
- Minimization of externally available services
- No user login possible; only device to device communication
- Secure encrypted communication
- Secure firmware update via signed updates

Other Zigbee devices such as, sensors, drivers or switches are devices that measure, receive and send data within the wireless lighting network. The devices feature the following security measures:

- No hardware debug interfaces available
- No user login possible; only device to device communication
- Secure firmware update via signed updates
- Encrypted network traffic (by default in Zigbee devices)

Load Controllers

Load controllers provide a connection between the wired field network and lighting control outputs. Although physical access to the lighting control devices cannot be entirely prevented, following the project installation guide and the associated Installation instructions for each lighting control device mitigates the risk.

Load controllers and lamp drivers must be installed in an approved enclosure with access restricted to electrical installers and facility management.

To maximize system security, the control cabling for field buses such as the Ethernet, RS-485, 1-10 V, DALI, and DMX bus must have restricted physical access (for example, concealed in the wall or ceiling space and requiring tools to gain access).

Devices feature the following security measures:

- No hardware debug interfaces are available
- Encrypted IP communications
- Signed secure firmware updates are deployed (platform specific, some limitations apply)
- Hardened operating system
- Minimization of externally available services
- No user login possible; only device-to-device communication

Sensors, User Interfaces and dry contact devices

Sensors, user interfaces and dry contact interfaces are devices that control, measure, and send/receive data.

To maximize system security, physical access to these devices and network cabling shall be restricted as much as practically possible and appropriate for the application. It is the responsibility of the system designer, installer, and end customer to ensure the required level of security is achieved in system design and installation.

Correctly installing devices by following the project installation guide and the associated Installation instructions for each lighting control device mitigates the risk.

These devices feature the following security measures:

- No hardware debug interfaces are available
- No user login possible; only device-to-device communication
- Only signed secure firmware updates are deployed (except for DDRC810DT-GL, DUS804CS-UP & DDMIDC8)
- RS-485 subnetworks firewalled by the Ethernet gateway or Ethernet enabled load controller.

The PDTS is the exception as user authentication is available:

- User authentication security - can be enabled so that logins are requested on touch-wakeup and a logout button is made available from the main menu.
- Tiered access levels - 0 (Guest) to 4 (Admin) - can be enabled per page, so that login is required to leave standby and/or to access restricted functions. A logout button can be added to any page.
- Restricted settings - The Settings page allows Guest users to temporarily lock the screen for cleaning, while Level 1-3 users can also reset their own password PIN. Device configuration and user management options are visible only to Admin users.
- Privacy - the PDTS cannot record or monitor user activity using the default or Maker UI. This may not apply to third-party created UIs. Additionally, the microphone is disabled in firmware. There is no camera installed. Dynalite will provide notice if there are any privacy related changes.

There are no functional differences with or without security applied, so the PDTS can be configured as required with any combination of secure and guest-accessible pages and controls.

D Users must be created on the PDTS itself; they're not associated with the 'Users' editor in SB.

4.1 Firmware updates

Installed device firmware can be upgraded on demand by the customer when there is a new firmware version. Firmware update frequency depends on the device type, problem reports and new feature

requests from customers. To ensure the highest level of security is maintained and features are up to date, it is recommended that all devices be upgraded to the latest firmware.

Device firmware and configuration can be updated over the network from System Builder by opening the job or database and saving to selected devices.

- A firmware update deployment starts with a secure, signed, and encrypted firmware file which is then deployed to all selected devices.
- A configuration update deployment starts with a modified device configuration in the config database, which is then deployed to all selected devices.

4.2 Decommissioning

This section explains the decommissioning of Ethernet-enabled devices and Zigbee devices. These devices can store unique site credentials such as user account information, security certificates, and IP addresses.

To successfully remove this data and decommission these devices, they must first be factory reset. Afterwards they can be powered off and physically removed.

- The factory reset mechanism for the PDDEG-S requires disconnecting the device from its power supply, removing the front cover, moving a jumper wire on the PCB to the reset position, replacing the cover and then powering up the device. The device must be powered down again and the jumper restored to the default position for operation.
- The factory reset mechanism for the PDEG, PDEB, DDRC-GRMS-E, DDBC320-DALI, PDTS and PDZG-E requires System Builder to perform a Device Factory Reset with the relevant options configured to delete certificates and delete IP addresses. The device can then be disconnected from its power supply.
- Zigbee devices store the credentials unless they are removed from the cloud platform.
  To successfully decommission Zigbee devices, they need to be removed from the cloud platform and the network. Afterwards they can be powered off and physically removed.

Any custom webpages should be removed from PDDEG-S, PDEG and PDTS.

When removing the PDDEG-S and PDEG from their intended environment, it is recommended to remove the SD-Card as it contains log information.

D Decommissioned non-Ethernet enabled devices do not store any security-related configuration data.

4.3 Product replacement

All devices can be reprogrammed by saving their configuration from the System Builder job or System Manager Config database.

Replacement Ethernet gateway/bridge - use new passwords and credentials for replaced devices.

Replacement DDRC-GRMS-E Room controller - for a specific system, saving the security certificate and configuration data, then setting the same DIP switches on a replacement room controller enables it to function identically to the replaced room controller. It is recommended that spare room controllers be kept in a secure location.

Replacement DDBC320-DALI, controller - for a specific system, saving the security certificate and configuration data enables it to function identically to the replaced DALI controller. Spares can be ordered from Dynalite.

Replacement DACM with multiconfiguration - for a specific system, setting the same DIP switches on a replacement user interface with the same multiconfiguration enables it to function identically to the replaced user interface (Antumbra or Revolution). It is recommended that spare user interfaces be kept in a secure location.

5 Cloud services

Connecting the lighting system to the Dynalite cloud platform provides multiple benefits such as configuration backups, secure job file sharing and remote maintenance. System security is given top priority from the specification phase, through to the hardware lifespan of each installation.

In accordance with our Security Development Lifecycle (SDL), Signify takes the following actions during product design, development, and testing:

- A security risk analysis, based on Signify security requirements aligned with the ISA/IEC 62443 standards suite, is performed for every new project and for every significant change to an existing project.
- Automated code analysis and manual code reviews are regularly performed during development. These analyses and reviews are based on, but not limited to, such frameworks as OWASP IoT Project and the OWASP Top Ten Project.
- Third-party code, including open-source code, is automatically analyzed to identify and mitigate vulnerabilities.
- Hardening of the operating system is performed for embedded devices and cloud-based solutions.
- Appropriate network security and firewall rules are implemented and reviewed regularly.
- Encryption of data in transit and at rest, when necessary, is implemented according to generally accepted industry standards.
- Penetration tests by internal and/or external parties are performed at regular intervals.

The Innovation team is responsible for evaluating the latest IoT security technologies and supports the development team in making the right choices when introducing new security algorithms, solutions, and technology partners.

Signify regularly audits its partners and supply chain to maintain the appropriate level of security in the manufacturing process.

5.1 Encryption and key management

Interact software uses only NIST-approved encryption algorithms, which ensures that only strong cryptographic algorithms are used. In-transit data between the PDDEG-S and the cloud platform is fully encrypted with TLS 1.2 or higher.

When the PDDEG-S is used in a project, data between PDDEG-S, Cloud platform and data traffic between the PDZG-E and PDDEG-S is encrypted using TLS 1.2 or higher.

The Zigbee network traffic, between the PDZG-E and lighting components, such as sensors, drivers or switches, is encrypted using 128-bit AES key. The security framework is defined in IEEE 802.15.4.

5.2 Business continuity

Dynalite cloud applications are offered as a Software-as-a-Service (SaaS), which is at the core of the Interact business model. Its services are stored in multiple locations. Backups and other data are stored in various availability zones, in accordance with data jurisdiction requirements to maintain a high level of business continuity.

Cloud services run on a highly available cloud infrastructure that enables continuous operation. In case of hardware failure, automatic changeover guarantees continuous operation.

Dynalite Cloud Connect delivers overall system security by conducting strict operational and account management processes. Monitoring the traffic and identifying threat situations that belong to regular operational processes are further key processes.

For all these operational processes, dedicated failover and disaster recovery plans are in place. These plans ensure that, in the unlikely event of an outage, the complete system can be restored.

5.3 Authentication and authorization

An identity management system is used to control access to the cloud platform.

It also applies when a specific service requires access to storage. For example, a third-party service needs to authenticate to access data or services in the cloud.

The authentication for APIs is done via OAuth 2.0 protocol using a set of credentials, namely a username and a password. The authorization endpoint returns a generated JSON Web Token (JWT) which is later used to authenticate when making calls to other endpoints.

The server implementation complies with the best practices of OAuth 2.0. It is required that each client is implemented respecting the same security requirements and recommendations as described in the OAuth 2.0 security best practices.

The identity management system also manages users and privileges. Users are invited to the system and assigned a role(s). Based on their role(s), users are assigned to customers or even to a more granular level such as access only to a group of sites.

Two-factor authentication (2FA) is available, depending on the federated identity management system used, and can be enabled for all users.

Service-to-service communications are secured by requiring a service principal authentication. The service principal comes from applications registered on Azure Active Directory, along with a secret and the scopes needed for each service-to-service communication.

5.4 System updates

Internally, mature software development and release procedures guarantee the high quality of Dynalite software.

Frequent software releases ensure that vulnerabilities are addressed in a timely manner.

All releases are thoroughly tested at different levels to prevent accidental data modification and to provide data consistency. This also includes security related test cases.

6 Data Classification and Inventory

Data gathered pertains to area usage by occupants. This includes the state of lighting scenes, motion sensor and light sensor data, temperature/humidity, and user interface interaction.

Devices do not store or process any personal data, however the system does provide state information from areas that, if linked to personally identifiable data (of the occupant or tenant), can be considered personal information. Hence, it is the system owner/operator's responsibility to secure and handle any personally identifiable data with confidentiality, in accordance with local legislation.

The system stores data in the following databases.

Data Assets	Description	Classification	Data Location(s)	Processing Time	Retention Time	Retention Category
Config DB	System and device configuration data (may include floorplans, background images). Site metadata: Site name, description, location, time zone. Customer metadata: may be stored in notes section. User identities and roles: authorization levels mapped to LDAP user IDs. Site control data: Schedule control, preset control, change management logging. SMTP server account details for email alerts.	Confidential	SM Server	customer decision	customer decision	customer decision
Trend DB	Status and history of the system, metrics (energy, motion, ...)	Confidential	SM Server	customer decision	customer decision	customer decision
Alarms DB	Status and history of the system, including online/offline status of devices, alarms, events, user logon/off.	Confidential	SM Server	customer decision	customer decision	customer decision
DataAccess DB PostgreSQL	Metrics (energy, motion, ...) used in APIs and on the Energy/System Dashboard. Site metadata: Site name, description, location, time zone.	Confidential	SM Server	customer decision	customer decision	customer decision
System credentials	Credentials and identities of services and devices, needed for establishing and maintaining system connectivity.	Secret	SM Server	customer decision	customer decision	customer decision

Additionally, the system also stores:

- Network log files on SM server and PDEG/PDDEG-S
- Application log files on SM server (DataAccess, OPC) and PDDEG-S

7 Compliance to (International) Standards

Signify is the first lighting company to be awarded the IEC62443-4-1 cyber security certification for our connected lighting development process. The certification lets potential customers, partners, and other stakeholders know that we are adhering to best practice in the security of our innovations, products, systems, and services.

The Signify Corporate Risk Management System is based on several industry standards adapted to Signify business objectives and strategy. Among others, our internal standards are aligned with the NIST Cybersecurity Framework, IEC 62443 standards, and the ISO 27000 series.

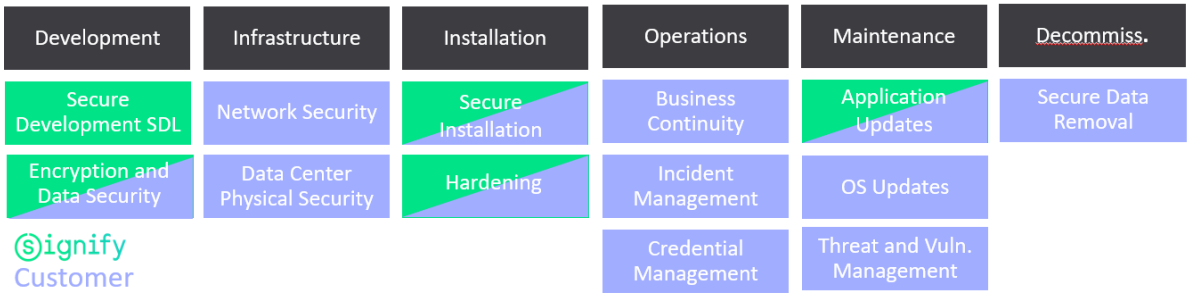
In terms of data protection of storage and privacy, Signify complies with GDPR: https://www.signify.com/global/legal/privacy/legal-information/privacy-notice

See the General Product Security Statement https://www.signify.com/global/product-security/professional-systems-and-services for more information.

8 Shared Responsibility Model

A typical Dynalite System only has on-premise components. Responsibility for security is typically shared between the manufacturer (Signify) and the Customer/Certified System Integrator (CSI).

Responsibilities for on-premise components



8.1 Responsibilities

Shared responsibility is regulated on a project basis with each customer via legal contracts. Measures to mitigate security risks are also taken on a project basis, depending on the requirements.

These are the typical shared responsibilities between Signify and the Customer/Certified System Integrator. Typically Signify provides the feature which can then be implemented by the Customer/CSI:

- Securing the installation, hardening and use of SM server.
- Integration with third-party systems, such as access control or building management systems.
- Implementation of industry protocols such as OPC and BACnet.
- Maintenance of network components.
- Physical security of network components, such as placement of the Ethernet gateways in an IT cabinet, or accessibility of load controllers in an electrical enclosure.
- User access security policies such as role-based access control and password changes.

The data and responsibilities below are for reference only. Each system may have different requirements and activities.

	Responsibility for on-premises components	Phase	Signify	Customer/CSI	Third-party
1	**User Credentials Management**				
1.1	Create new accounts	Operation		R A	
1.2	Update accounts	Operation		R A	
1.3	Delete accounts	Operation		R A	
2	**System Keys Management**				
2.1	Generation	Installation		R A	
2.2	Storage	Operation		R A	
2.3	Sharing	Operation		R A	
3	**Certificates (web)**				
3.1	Provisioning	Operation		R A	
3.2	Renewal	Operation		R A	
4	**Application Management**				
4.1	Update/Upgrade	Operation		R A	
4.2	Configuration	Installation		R A	
5	**Infrastructure / OS Management**				
5.1	Installation	Installation		R A	
5.2	Hardening (if Signify delivers server + OS)	Installation	R A		
5.3	Hardening (if customer delivers server + OS)	Installation	C	R A	
5.4	Patching / Maintenance	Operation	C	R A	
5.5	DB Hardening	Installation	C	R A	
5.6	Web Server Hardening	Installation	C	R A	
6	**Licensing**				
6.1	External Components License Provisioning	Installation		R A	C

	Responsibility for on-premises components	Phase	Signify	Customer/CSI	Third-party
6.2	External License renewal	Operation		R A	C
7	**Backups**				
7.1	Backup Procedure	Installation		R A	
7.2	Configuration / Data Backup	Operation		R A	
8	**System Development**				
8.1	Hardening	Development	R A		
9	**Network**				
9.1	Router Configuration	Installation		R A	
9.2	Update	Maintenance		R A	
9.3	Patching	Maintenance		R A	
10	**Monitoring**				
10.1	Scanning for intrusion/malware	Operation		R A	I
10.2	Performance monitoring (availability)	Operation		R A	I
11	**Incident Management**				
11.1	Report			R A	I
12	**End Point Protection**				
12.1	Antivirus License			R A	
12.2	Antivirus installation			R A	
12.3	Other End point protection			R A	

R Responsible - Those who do the work to achieve a task. The person who does something to execute a specific task or activity.

A Accountable - Those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom Responsible is accountable.

C Consulted - Those who are not directly involved in a process but provide inputs and whose opinions are sought.

I Informed - Those who receive outputs from a process or are kept up to date on progress, often only on completion of the task or deliverable.

9 Secure Installation Requirements (for customers)

Securing the system at all points of connection is critical to installing technology across the building. To mitigate risks, it is recommended to implement the following security measures:

1. Physical and/or logical separation of the lighting network from other IP networks.
2. Restricted physical access to control network devices and cabling.
3. User management tools using role-based access controls.
4. Secure communications between Ethernet devices.
5. Secure communications to the System Manager API.

Physical and/or logical separation of the lighting network

The system typically uses the existing IT infrastructure for multiple services. Therefore, it is recommended to install the system on a separate VLAN to limit security issues with IP address ranges provided by the customer. Ethernet enabled device firewalls provide separation between the IP network and the RS-485 field network.

Restricted physical access to control network devices

All devices delivered on- site that are manufactured by Dynalite must be accounted for before being installed by the electrical contractor.

The Ethernet network for the lighting control system should be physically inaccessible to unauthorized persons, thus isolating and mitigating any external security risks.

Physical access to the PDZG-E wireless gateways can't be completely prevented as they are attached to the wall or ceiling and spread across the building, thus falling under shared responsibility. This is the reason why these devices need to be prevented from accessing resources on the corporate IT network.

User management tools using role-based access control.

The System Manager Configuration app is used to configure access to the SM client application. User authorization is configured by the super administrator user who adds Users, roles, permissions, and tenancy access. When using a domain, Windows users can be linked to their employer's corporate LDAP services for user account control. We recommend the use of strong passwords.

Secure communications

The PDDEG-S Ethernet gateway and Ethernet enabled load controllers must have a security certificate installed to securely connect to each other and to the SM server via the IP network and without internet connectivity.
In-transit data between the System Manager server and the PDDEG-S Ethernet gateway is fully encrypted over a TCP TLS connection. The TLS connection is established using a device specific certificate and private key.

Traffic between the PDDEG-S Ethernet gateways and Ethernet enabled load controllers is also encrypted over a TCP TLS connection. The TLS connection is established using a site-specific certificate chain.

The system is designed to prevent a potential attacker gaining unauthorized access to data or control over the system.

Default secure port numbers for Ethernet-enabled devices:

- Port 51443 for secure TCP TLS trunk connections (System Manager - Ethernet Gateway)
- Port 50443 for secure TCP TLS floor connections (Ethernet Gateway – Ethernet enabled load Controller)
- Access to the inbuilt webserver should be secured via HTTPS. PDDEG-S only supports HTTPS. PDEG supports HTTPS and HTTP (HTTP webservices are supported for backwards compatibility only).

System Manager API

Authentication for the System Dashboard web site is not configured by default. Customers are encouraged to configure authentication as described in the Lighting API Online User Guide.

Authentication for System Manager APIs is handled via Windows Authentication using a set of credentials, namely a username and a password. The client makes the request using basic authentication, and the server validates the credentials against Windows users that are configured locally on the server machine or centrally in Active Directory.

The server implementation complies with the best practices of OAuth 2.0. Each client must be implemented respecting the same security requirements and recommendations as described in the OAuth 2.0 security best practices.

To maximize security, the system dashboard design and deployment follows best practice guidelines (OWASP).
Administrators can set up app credentials for the dashboard and other third-party interfaces to access the API.

As part of the handover of the system to the customer, the customer's IT team configures HTTPS access to the API by installing a TLS certificate (the API cannot be used without this). This can be performed in one of two ways:

1. **Customer provides certificate (recommended).**
    1. Customer's IT team sends a certificate signing request to a certificate authority to sign, or they may use an existing certificate.
    2. This allows reuse of existing customer domains and certificates, meaning the certificates are fully managed and controlled by the customer.
    3. The customer's IT team needs to issue the certificates to Signify for use on the SM server, in line with the IP/subdomain they assign to the control system.
    4. The customer's IT team needs to match this in their DNS tables or distribute it to each client PC's hosts file.

2. **Signify provides certificate.**
    1. Signify can issue a self-signed certificate (Dynalite as the authority) for system services.
    2. As well as installing on the SM server, the customer's IT team must distribute this certificate to all client PCs that need to access system services.
    3. The domain used is fictitious, (e.g. "https://philips.dynalite/") and requires the customer's IT team to match this in their DNS tables or distribute it to client PCs' hosts files.

9.1 Additional hardening requirements

In case the Windows server is supplied and operated by the customer, the customer IT team is responsible for proper hardening, operation, and maintenance of the server.

In case the contract for the system requires Signify to provide the Windows server, Signify will harden the server to our internal hardening specifications. Responsibilities for operation and maintenance must be agreed upon in the contract.

D For more information, please refer to the OS Hardening Guide.

9.2 Security Configuration options

The system uses 2048-bit RSA keys and AES 128-bit keys to authenticate and encrypt network traffic from the SM server, PDDEG-S Ethernet gateways and Ethernet enabled load controllers.

Every available service on a server introduces a certain security risk. Naturally, some services are required for a server to perform its primary function. However, services that are not required should not be left publicly available, as an attacker may be able to exploit potential vulnerabilities in the services provided to gain unauthorized access to the system. Therefore, all devices running Dynalite software should be hardened to minimize attack surfaces and vectors.

The following ports may be required for the proper functioning of the system:

Device	Port and Protocol	Description
System Manager server machine (Windows)	3260 HTTPS & WSS	For the Energy/System Dashboard, REST APIs, and websocket.
	3389 RDP	For remote desktop connections
	8084 WCF	Required for SM clients to connect to SM server.
	25 (StartTLS), 587 (StartTLS) or 465 (Implicit SSL) SMTP Client	For outbound communication with SMTP server.
	8734 WCF	Port 8734 is required for System Manager connection to the Data Access service and must not be used by another service. Data Access usually resides on the same server, so a firewall rule is not required.
PDDEG-S	80 HTTP.	Required to display the open-source license page.
	443 HTTPS.	For secure webpages, firmware upgrades and API.
	50443 TCP TLS Server.	For secure Ethernet spur/ inter-spur connections.
	51443 TCP TLS Server	Required for secure Ethernet trunk connection.
	5353 IGMP	Required for mDNS.
	123 NTP Client	Network Time Protocol used to synchronize real time clock from the internet.
PDEG/PDEB	50000 TCP Server	For unsecure Ethernet trunk connections.
	50001 – 50003 TCP Server	For unsecure Ethernet spur/ inter-spur connections.
	443 HTTPS Server	For secure webpages, firmware upgrades and API.
	5353 IGMP Client	Required for mDNS.
	123 NTP Client	Network Time Protocol used to synchronize real time clock from the internet.
DDRC-GRMS-E	50443 TCP TLS Client	For secure gateway connection. (Gateway Mapping Port).
	5353 IGMP	Required for mDNS.
DDBC320-DALI	50443 TCP TLS Client	For secure gateway connection.
	5353 IGMP Client	Required for mDNS.

D System hardening is recommended since other ports may be opened at the discretion of the commissioning technician.

9.3 Instruction and Recommendation for Security Tooling

Not Applicable

9.4 Security Maintenance Activities

Philips Dynalite systems include:

- Software and firmware updates provided regularly throughout the licensed period. Updates are customer installed unless otherwise included in a lifecycle package.
- APIs (with features matching the System Manager license model). These can be activated on request at no extra charge.
- An optional maintenance contract to upgrade and check system performance, and provide software, security, firmware, and configuration updates.

9.5 Security Mitigation

Measures to mitigate security risks are taken on a project basis, depending on the requirements. Typically, integration with a third-party system may require the use of an unsecure communication protocol.

For example: Connectivity to Industrial controls, SCADA and building management systems is often implemented via protocols such as Modbus or BACnet. Although there are ongoing efforts, these protocols often do not provide secure alternatives or if they do, they may not be implemented by every device. Therefore, alternative mitigating controls should be implemented. Such alternatives are usually in the form of a Secure VPN tunnel. Although this is not fully encrypted end to end, it often provides an appropriate level of protection (residual risks should still be evaluated).

10 Security Operations Requirements (for Customers)

Technical and process security features are implemented in all Philips Dynalite projects to minimize security issues, such as pre-programmed devices, inbuilt firewalls, restricted set of protocols, encrypted connections, and user authentication.

10.1 Accounts on server and devices

Unique usernames and passwords are required for the following accounts:

Microsoft SQL Express Database

- Superuser is setup during SM installation to allow SM to access the Data Access (MSSQL) Database.

PostgreSQL Database

- PostgreSQL is used for Data Access/System Dashboard.
- PostgreSQL must be installed separately, and super user password configured before SM installation. User must enter superuser password during SM installation to allow SM to create a less privileged user 'DataAccessUser' to access the Database.

System Manager Configuration

- The System Manager Configuration application can only be run locally on the SM server machine by a logged-in Windows user. It cannot be run remotely.

System Manager Client

- The SM client is initially installed on the server with only the designated site administrator user. Multiple SM clients may be required in the system for different users. The SM client uses Windows users' accounts to authenticate, and role-based permissions assigned in the SM Configuration app. Windows users may be configured locally on the SM server or centrally in Active Directory.

System Dashboard

- No authentication by default. Authentication can be configured as described in the Lighting API Online User Guide.

Lighting API

- Windows user authentication on the APIs, validated against Windows users configured locally on the SM server or centrally in Active Directory.
- No authentication on the events websocket.

Ethernet Gateways

- A Username and default password is set up in all Ethernet Gateways for the web server option. Password is supplied on a sticker in the box. The commissioning process instructs commissioning engineers to create a unique password in each Ethernet Gateway (> 20 character fully random, that is not shared by any other gateway). If not used the webserver must be disabled during commissioning.
- User accounts and passwords should be unique and are hashed in each gateway, limiting potential access. In the unlikely event of one gateway being compromised, the others will remain unaffected.
- The PDDEG-S can be configured for user authentication using LDAP, or OAuth 2.0 for external management of user accounts.
- Certificates are encrypted on the PDDEG-S. Philips Dynalite software uses only NIST-approved encryption algorithms, ensuring that only strong cryptographic algorithms are used.

11 Security Maintenance Requirements (for Customers)

System updates

Firmware and device configuration updates can also be deployed by the customer's representative or Certified System Integrator (CSI) representative.

Internally, mature software development and release procedures guarantee the high quality of the System Manager software. Frequent software releases ensure that potential vulnerabilities are addressed in a timely manner.

All releases are thoroughly tested to prevent accidental data modification and to provide data consistency. This also includes security-related tests applied during the system release, test and validation process.

Signify provides helpdesk & remote support and can also offer a customized service agreement as part of the system to optimize maintenance activities.

Business continuity

To maintain overall system security, the customer must provide strict operational and account management control processes. Monitoring traffic and identifying threat situations are regular operational processes that are the responsibility of the customer's local IT team.

System Manager runs on a local server. To mitigate risk of potential hardware failure, an alternative server machine plus OS support and configuration backup and redundancy may be set up by the customer's IT team to ensure continuous operation.

System Manager services can be stored in multiple locations. Backups and other data should be stored in various availability zones, in accordance with data jurisdiction requirements, to maintain a high level of business continuity. For all operational processes, there should be local dedicated failover and disaster recovery plans. These plans ensure that, in the unlikely event of an outage, the complete system can be restored.

12 Security Incidents

Signify addresses security as an integral part of our quality process. Assigned responsibilities and established procedures ensure an adequate response to suspected security events and incidents. Each suspected security event is assessed against a set of criteria to determine whether it qualifies as a security incident. When security incidents occur, immediate and appropriate mitigation measures are taken.

Lessons-learned activities are conducted periodically, and additionally after major incidents, to improve security measures in general and incident handling in particular.

We expect customers to proactively inform Signify if there is any indication of a potential security incident. Security incidents should be communicated to our Customer Satisfaction Team.

It is important that actual or suspected security incidents are reported as early as possible.

12.1 How to report a Security Incident

Security Incidents and Events should be reported to Signify via the Customer Satisfaction Representative. Security Incidents will be handled by our Security Team and customers will be kept informed.

Confirmed incidents (for example, breach of Signify systems) will be shared with impacted customers within 3 days of the confirmation of the breach. We will follow reporting according to the GDPR regulation to additionally report incidents which involve Personal Data

Signify will collaborate with customers for reasonable additional investigation when formally requested.

See the General Product Security Statement for more information https://www.signify.com/global/product-security/professional-systems-and-services.

13 Coordinated Vulnerability Disclosure

Signify supports responsible vulnerability disclosures and encourages researchers and ethical hackers to report identified vulnerabilities.

13.1 How to report a vulnerability

For more information on Signify responsible disclosure, visit our *Coordinated vulnerability disclosure page*.

14 Known Vulnerabilities and Security Advisory

Vulnerabilities are classified according to the CVSS framework: https://www.first.org/cvss/calculator/3.1

Common Vulnerability Scoring System Version 3.1 Calculator https://www.first.org

Security vulnerabilities are handled within our Security Development Lifecycle, and we share with the customer through our Security Advisory Page.

Known vulnerabilities, mitigations and workaround are published on our Security Advisory page:

https://www.dynalite.com/security-advisory/

15 Legal Disclaimer

This information represents the current product security information as of the date of publication but is provided “as is” without warranty of any kind, whether express or implied. This information is subject to change without notice.

Customers are responsible for making their own independent assessment of Signify products or services and their use thereof. Any commitments or liabilities in respect hereof are defined in the agreements between Signify and its customers.

R07, 10 December 2024

Philips Dynalite

www.dynalite.com