PHILIPS
dynalite
Controls

Security Statement

Contents

1 Introduction

1.1 Security aspects

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

This document's purpose is to describe the security measures built into the architecture, and to address product security concerns that customers might have.

As connected lighting systems are an integral part of the Internet-of-Things (IoT), they are also associated with 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 internal networks. Company-issued computers, smartphones, tablets, and so on are considered attack vectors and must comply with certain rules in order to be trusted and granted access to internal corporate networks. The same procedures apply to IoT systems connected to a corporate network.

The key concerns regarding IoT solutions deployed on a corporate IT 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 platform's security aspects by providing:

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

1.2 System building blocks

The Dynalite platform has a wide range of applications with many inbuilt features, such as networked user interfaces, multifunction sensors, lighting control, motor control and HVAC control. Hardware and software gateways support a choice of standard industry protocols and integration options. 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 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, and analytics for an entire building or group of buildings.

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

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

The Philips Dynalite portfolio consists of the following building blocks:

Hardware	• Network integration devices • User interfaces • Light intensity and occupancy sensors • Load controllers (Switching, Signal dimming, Phase-cut dimming, Multipurpose)
Software	• System Builder commissioning and design software • System Manager software suite, (Configuration Tool, SM Client, Desktop Switch App, System Dashboard, and API for third-party interfaces) • Mobile control apps
Integration	• API-based integrations • Software gateway integrations using industry standard and proprietary protocols (such as, FIAS, SMTP, Access Control, OPC). • Hardware gateway-based integration. DyNet1 and DyNet2 to: 1-10V, DSI, DALI, DMX, KNX, LON, BACnet, Modbus, Somfy, Hue, USB, Bluetooth, Infrared (RC5), IP (TCP, UDP, FTP, Telnet, Text over IP). • Cloud services: Interact Office, Interact Retail HQ.

1.3 Glossary

Term	Description
AES	AES is a symmetric key encryption scheme, which relies on a 128-bit shared secret key used for encryption and decryption of network data.
API	Application Programming Interface. The System Manager API provides access for the browser-based dashboard and third-party interfaces to system data.
Area	A logically defined space in a building, such as a room, or part of a room.
BMS	Building Management System.
Dashboard	Browser-based System Dashboard.
Data Access	A System Manager service, to support APIs and web servers.
DDBC320-DALI	Philips Dynalite DALI-2 three universe driver controller
Devices	Philips Dynalite hardware, such as load controllers, sensors, user interfaces etc.
EG	Ethernet Gateway (a PDEB, PDEG or PDDEG-S)
DDRC-GRMS-E	Philips Dynalite Ethernet-enabled field device that provides a secure Ethernet connection between a floor Ethernet gateway and RS-485 room devices. Integrates IP network to RS-485 subnetwork and provides load control and I/O functionality within a room.
IDS	Intrusion Detection System.
IGMP	Internet Group Management Protocol. A communication protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
IPS	Intrusion Prevention System.
IPTV	Internet Protocol-based Television.
LDAP	The customer's Lightweight Directory Access (client-server) Protocol for accessing directory services.
mDNS	Multicast DNS.
MFA	Multi-Factor Authentication.
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PDDEG-S	Philips Dynalite DIN rail Ethernet Gateway – Supervisor. Provides secure IP integration between System Manager and cloud, DDBC320-DALI, DDRC-GRMS-E and between EasyAim devices.
PDEG/PDEB	Philips Dynalite Ethernet Gateway/Bridge providing IP to RS-485 DyNet integration between SM and spur devices.
PDTS	Philips Dynalite Touchscreen
RDP	Remote Desktop Port.
SB	Philips Dynalite System Builder.
SDL	(Signify) Security Development Lifecycle.
SIEM	Security Incident Management System.
SM	Philips Dynalite System Manager.
SMTP Server	(Customer's) Simple Mail Transfer Protocol server for sending notification emails.
Websocket	A websocket provides a long-held streaming connection between the client and server which allows for bidirectional, full duplex, event-driven messages without having to poll the server.

2 Security principles

Philips Dynalite systems are typically managed by the customer and their local IT support. This includes backup, logging, monitoring, and management of device statuses, logical area statuses, setting changes and alerts. Our systems do not store building occupant's personally identifiable data, only anonymous logging of system events and usage statistics.

System security is given top priority from the specification phase, giving due consideration to the hardware lifespan of each installation.

All our internal and external development activities follow the Signify Security Development Lifecycle (SDL), which codifies industry-accepted best practices. The major components of the SDL are security risk analysis and threat modeling, code analysis and review, and vulnerability management. We apply the SDL to all our hardware products, systems, services, software, and cloud solutions.

At Signify we implement a security policy that enforces segregation of duties and applies least-privileged access principles

Signify development teams and other personnel in general do not have access to commissioned systems or production data. When access to data is necessary to support operations, only the authorized team is allowed, and strictly for the limited time and scope needed.

More information about the security principles used by Signify can be found in the General Security Statement:

https://www.signify.com/global/security-and-privacy- statement-for-connected-products

3 Architecture and Security

Philips Dynalite products are designed for on-premises systems based on our modular controls architecture. Devices are usually connected in a trunk-and-spur topology, with the System Manager head-end software and gateways connected to the Ethernet or RS-485 trunk network. Gateways then typically connect to the RS-485 spur devices on each floor. The 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.

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.

Devices communicate with each other on the field network using the DyNet protocol and operate independently of the System Manager head-end software. 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:

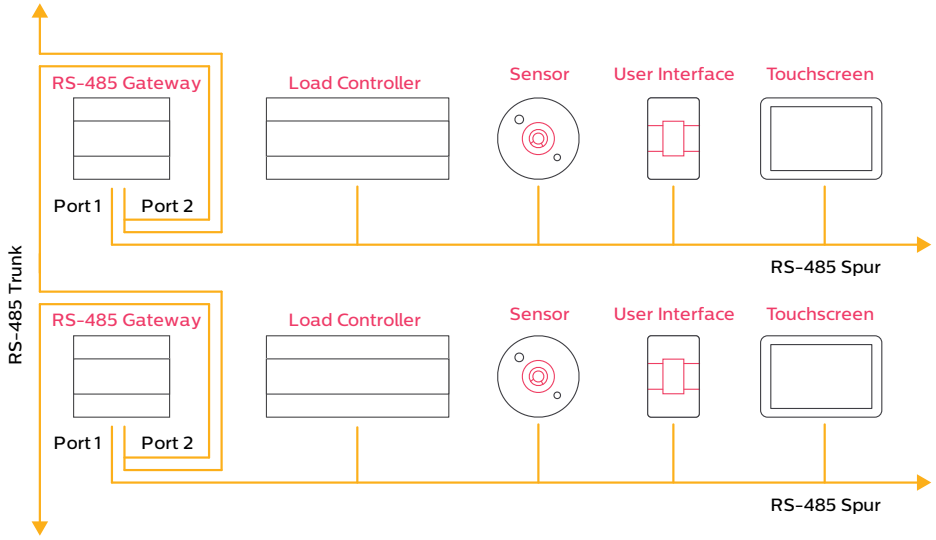
1. RS-485
2. Ethernet

3.1 RS-485 connections

Most Dynalite devices have an RS-485 port so they can be connected to the spur field network on each floor of a building. Gateways then connect the spur networks to the trunk network in the building. Although Ethernet trunks are used more frequently, a trunk and spur network can also be created with RS-485 gateways using an RS-485 trunk.

Ethernet gateways/bridges integrate the IP network with the RS-485 field network. They use authentication and network firewalls to ensure secure access and that only allowed messages are passed to the RS-485 field network. Access to the RS-485 field network occurs only via direct physical connection or via a gateway/bridge.

Gateways can be reconfigured, and factory-reset from the RS-485 network. Therefore, devices with RS-485 ports must be physically secured by installing in a secure enclosure/room, with wiring kept physically inaccessible to unauthorized personnel.



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

3.2 Ethernet connections

Ethernet (or optical fiber) is often used for the IP trunk network. An Ethernet spur may also be connected to other Ethernet devices. The Ethernet connection security depends on each device's capabilities. There are currently four Ethernet enabled devices in the product portfolio that provide gateway/bridging functionality to other parts of the system.

Ethernet Gateways

- PDDEG-S
- PDEB/PDEG

Ethernet enabled load controllers

- DDRC-GRMS-E
- DDBC320-DALI

PDDEG-S

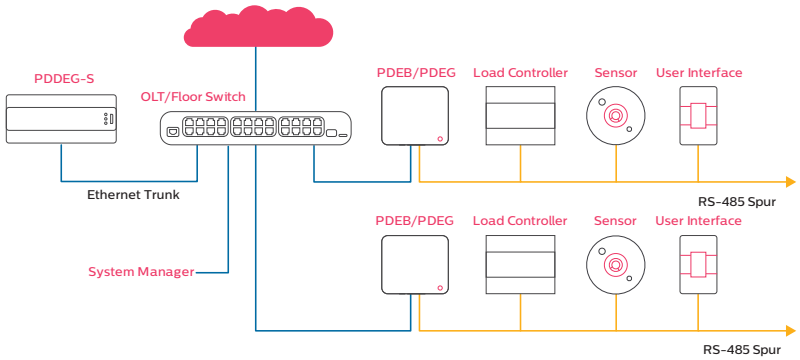
The PDDEG-S can be used for multiple functions in the system. The two most common functions are:

- Building Connectivity Bridge – providing a secure internet connection to the building.

  Internet access to a PDDEG-S is secured with Transport Layer Security (TLS 1.2 or later).
  The system can only be accessed remotely with an encrypted, authenticated connection.

  Network traffic between SM and the PDDEG-S is secured with a TCP TLS connection.
  The architecture uses a client/server relationship from the SM server to the PDDEG-S, ensuring that intruders on the IP network cannot initiate a connection to SM.

  The routing configuration in each gateway/bridge prevents intruders from controlling or intercepting traffic between spurs.

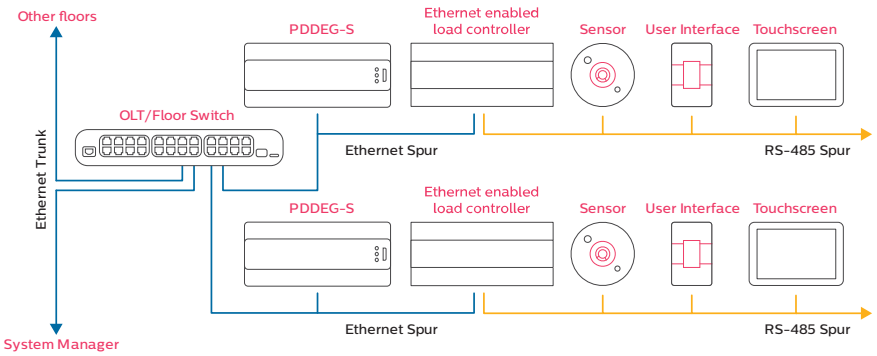


- Floor Ethernet Gateway – providing a network bridge between the Ethernet trunk and an Ethernet or RS-485 DyNet spur.

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

  Network traffic between PDDEG-S and an Ethernet enabled load controller is secured using a TCP TLS connection. 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 required physical network security measures in place. For more details, refer to the Ethernet Gateway Commissioning Guide and Interact Hospitality Commissioning Guide.

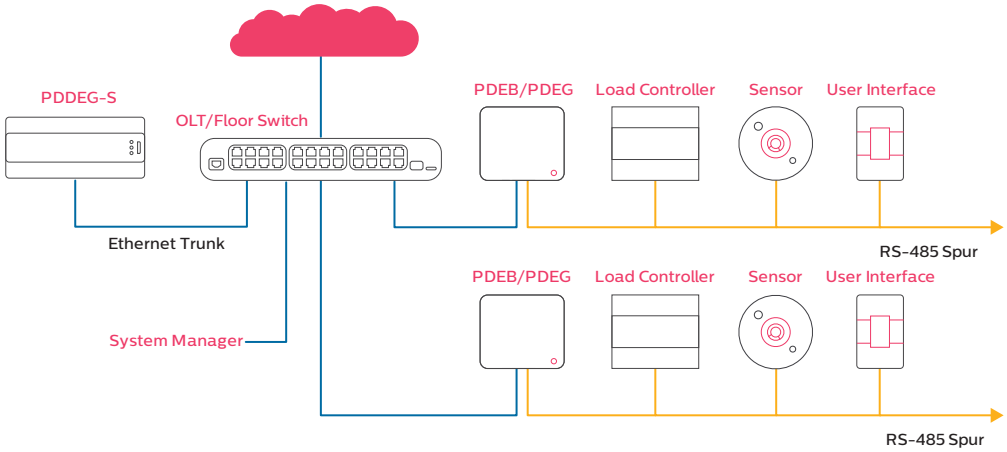


PDEB/PDEG

Network traffic between System Manager and the PDEB or PDEG is authenticated and (where required by the customer) it may need to be complemented 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 secured via HTTPS. There is no webserver on the PDEB.



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

The Philips Dynalite Touchscreen (PDTS) User Interface has an Ethernet port, that is used for configuration/maintenance purposes only. To maintain a maximum level of 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.

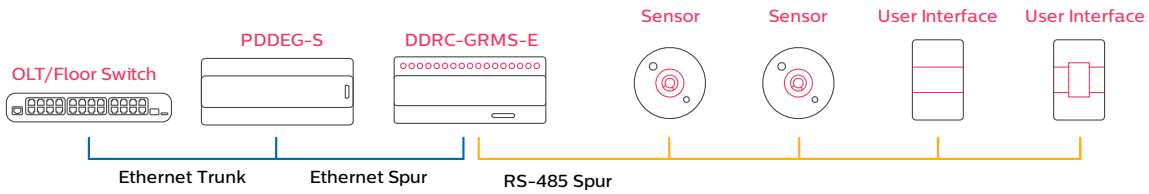
DDRC-GRMS-E

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 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.

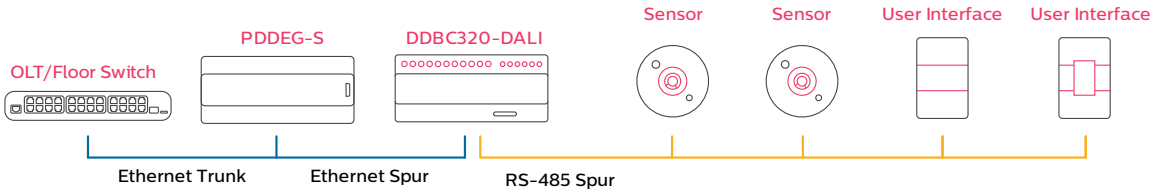
DDBC320-DALI

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.

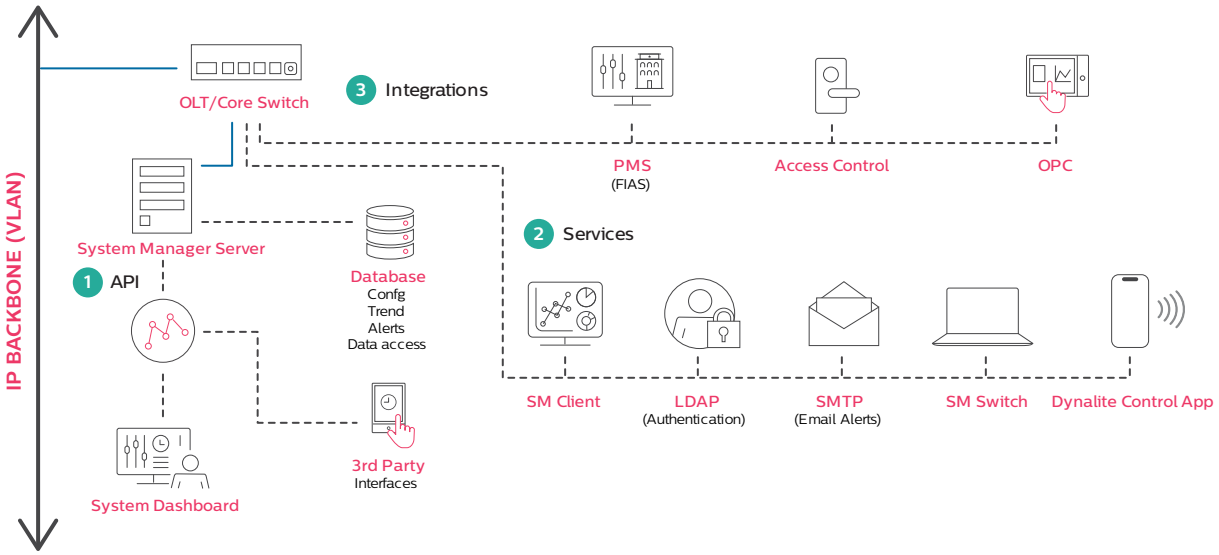
The DDBC320-DALI does not have any user accounts.



4 Network security

System Manager Connections

In addition to being connected to the control system field network, System Manager is also connected to the corporate IT network enabling user and integration access. Each connection may have specific security implications and requirements.



4.1 API & websocket to interfaces

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 and use a HTTPS connection with basic authentication. For easy and secure login and password management, Microsoft Active Directory can provide user authentication.

4.2 SM to enterprise clients

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

- SM clients – Enterprise client app.
- LDAP – user management directory services.
- SMTP server – email notifications.
- System Manager Switch – desktop lighting control app.
- Dynalite Control app – control app for mobile devices.

4.3 SM to integrated systems.

System integration facilitates two-way communication for unified, sitewide intelligence with third-party network systems to exchange commands and data about system operation. Systems can be integrated using a relevant gateway device or the 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 often do not provide secure alternatives. Therefore, alternative mitigating security measures should be implemented. Appropriately securing user access to these systems is the responsibility of the customer.

The following Integrations are available:

Software gateways	Hardware Gateways (not shown in diagram)
PMS (FIAS protocol)	BMS/HVAC (BACnet)
Access Control (Saflok, VingCard)	KNX
OPC	Somfy

IP network connections

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 open ports are needed for the proper functioning of the system:

Device	Port & Protocol
(Windows) Web server	3260 HTTPS. For the System Dashboard 443 HTTPS. For connection to the Dynalite cloud platform. 3389 RDP (optional for Remote Desktop Connections). 8084 is required for SM clients to connect to SM server. 636 client. For secure outbound communication using LDAP over SSL (LDAPS). An alternative port may be configured. 389 client. For secure outbound communication using LDAP or LDAP+StartTLS. An alternative port may be configured. 25 (StartTLS), 587 (StartTLS) or 465 (Implicit SSL) client. For outbound communication with SMTP server.
PDDEG-S	80 HTTP. Required to display the open source license page. 443 HTTPS. For webpages, firmware upgrades and API. 50443 TCP TLS 1.2 server. For Ethernet Spur device connections. 51443 TCP TLS 1.2 server. Required for System Manager connection. 5353 IGMP. Required for mDNS. 123 NTP client port.
PDEG/PDEB	50000 – 50003 TCP. 443 HTTPS server. 5353 IGMP. Required for mDNS. 123 NTP client port.
DDRC-GRMS-E	50443 TCP TLS 1.2 client. EG connection (Gateway Mapping Port). 5353 IGMP. Required for mDNS.
DDBC320-DALI	50443 TCP TLS 1.2 client. EG connection. 5353 IGMP. Required for mDNS.

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

5 Device and physical security

This section on device and physical security describes additional measures to protect the system by prohibiting physical access to Ethernet gateway devices and field network devices. It is the customer's responsibility to ensure the appropriate level of unauthorized physical access prevention is always in place.

5.1 System Manager Server

System Manager provides the monitoring and management functions of the system. It is advised that the System Manager Server, through which all traffic is routed, 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.

5.2 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.

Each Ethernet Gateway provides a connection between the field network and the System Manager server. Ethernet Gateways authenticate with the 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

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

- Secure Ports
- 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
- MAC address
- Serial number
- Default username and password (default username and password must be changed upon installation)
- 12NC

5.3 Load Controllers

The controller provides a connection between the wired field network and the lighting control outputs. Although physical access to the lighting control devices cannot be entirely prevented, following the system 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, DALI, and DMX bus must have restricted physical access (for example, concealed in the wall or ceiling space and requiring tools to gain access).

The devices feature the following security measures:

- No hardware debug interfaces available
- Port security
- 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

5.4 Sensors and User Interface devices

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

To maximize system security, physical access to sensors, UIs 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 system 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 available
- No user login possible; only device-to-device communication
- Only signed secure firmware updates are deployed
- RS-485 subnetwork firewalled by the Ethernet gateway or Ethernet enabled load controller.

The PDTS is the exception as user logins are available if required for:

- 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. There are no functional differences with or without security applied.
- 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.

5.5 Firmware and software upgrades

Firmware of on-site devices can be upgraded on demand by the customer when there is a new firmware version. To ensure the highest level of security is maintained and features are up-to-date, all devices should receive the latest firmware upgrades.

Device firmware and configuration can be updated from System Builder by opening the SM Config 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.

5.6 Decommissioning

This section explains the decommissioning of Ethernet-enabled devices. These devices 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, replacing the cover and then powering up the device.
- The factory reset mechanism for the PDEG, PDEB, DDRC-GRMS-E, DDBC320-DALI and PDTS 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.

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.

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

5.7 Product replacement

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

Ethernet gateways/bridges, - use new passwords and credentials for replaced devices.

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.

DACM multiconfiguration - for a specific system, setting the same DIP switches on a replacement user interface with 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.

6 Security installation requirements

6.1 Security measures

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 control (for enterprise clients).
4. Secure communications between SM Server, PDDEG-S, DDRC-GRMS-E and DDBC320-DALI.
5. Secure communications to the System Manager API.

6.1.1 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. The Ethernet enabled device firewalls provide separation between the IP network and the RS-485 field network.

6.1.2 Restricted physical access to control network devices

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

All devices that are preconfigured by Signify must be accounted for before being installed by the electrical contractor.

6.1.3 User management tools using role-based access control.

The System Manager Configuration app is used to control access to the SM client app. User authentication is configured by the superadmin user who adds users, user profiles, permissions. and floor access. Optionally, users can be linked to their employer's corporate LDAP services for user account control. We recommend the use of strong passwords.

6.1.4 Secure communications

The PDDEG-S Ethernet gateway and Ethernet enabled load controllers must have a security certificate installed to connect to each other and to the SM server via a secure IP network without internet connectivity. 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 – Room Controller)
- Access to the inbuilt webserver should be secured via HTTPS (PDDEG-S supports HTTPS only. PDEG supports HTTPS and HTTP, however HTTP webservices are supported for backwards compatibility only).

6.1.5 Secure communications to the API

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.
    4. TLS certificates have a validity duration equal to the purchased license period and will only be renewed if the System Manager license is extended.

7 Operation

7.1 Accounts on devices

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.

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.

System Manager Configuration

- Superuser (Site Administrator)

System Manager Client

- The SM client is initially installed on the server with only the designated site administrator superuser. Multiple SM clients may be required in the system for different users. The SM client uses Windows users' accounts to authorize, and role-based permissions are assigned in the SM Configuration client.

System Dashboard

- Windows local user authentication or corporate LDAP service using LDAP + StartTLS.

Lighting API

- Windows local user authentication or corporate LDAP service using LDAP + StartTLS.

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.

7.2 Encryption and key management

Keys

Philips Dynalite software uses only NIST-approved encryption algorithms, ensuring that only strong cryptographic algorithms are used.

Certificates are encrypted on the PDDEG-S.

Encrypted communications

In-transit data between the System Manager server and the PDDEG-S Ethernet gateway is fully encrypted over a TCP TLS 1.2 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 1.2 connection. The TLS connection is established using a site-specific certificate chain.

7.3 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, a separate server machine plus OS support and configuration backup and redundancy shall 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.

7.4 Authentication and authorization

Authentication for third-party interfaces applies when a specific service requires access to data via the API and websocket. For example, a third-party service needs to authenticate to access data.

The authentication for System Manager APIs is handled 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. Each client must be implemented respecting the same security requirements and recommendations as described in the OAuth 2.0 security best practices.

7.5 System updates

Customer facility management teams can deploy updates to default variables such as occupancy timeout, temperature setpoint, lighting scenes, power socket state and window covering position.

Firmware and device configuration updates can also be deployed by the customer's representative or Value-Added Partner (VAP) 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 at different levels 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. Signify can also offer a customized service agreement as part of the system to optimize maintenance activities.

8 Privacy and data governance

Data gathered pertains to usage of the rooms/areas and devices by the occupants. This includes occupied state, state of monitored doors and curtains, temp/humidity data, lighting settings, current scene, and motion and light sensor data.

None of the devices store or process any personal data, however the system does provide state information from logical areas (as above) that, if linked to personally identifiable data (of the occupant or tenant), can be considered personal information. Hence, it is the System owner/operator responsibility to secure and handle with confidentiality any personally identifiable data, in accordance with local legislation.

The system stores data in the following databases:

- Config database
- Trend database
- Alarms database
- Data Access (MSSQL) database

8.1 System telemetry

8.1.1 Sensor data

Sensor data is generated by specific types of sensors within the room such as motion, light, temperature and humidity sensors, to control services in the area. It is also sent back to the head-end software.

The following data is sent by sensors:

- Occupancy
- Light levels
- Temperature
- Humidity
- Door/window open/closed status
- FCUC Filter Dirty
- FCUC Drip Tray Full
- Soil Moisture
- Water Leak

8.1.2 User Interface data

User interface (UI) data is generated by occupant button presses to control services in the area. It is also sent back to the head-end software.

The following data is sent by UIs:

- Temperature setpoint
- Preset scene control
- Lighting intensity control
- Color control
- Window covering control

8.1.3 Edge components status/data

All data is sent by devices to the SM server via a gateway and is stored in the Trending database. If sensor data exceeds configured parameters, then an associated alert is stored in the Alarms database. Network devices also send online/offline status to SM.

8.1.4 Logging and log monitoring – Audit trail

Ethernet gateways store a log of floor (spur) network events (i.e. messages sent and received on spur ports). Log files can be downloaded from the device via HTTPS or using System Builder's Manage Log Files feature.

Ethernet Gateway logs

- Log files are stored in an unencrypted format on device directory A.
- Log files are stored for up to 28 days before being overwritten.

System Manager logs

- Room events are logged and viewable on the Dashboard.
- Dashboard logs firmware, configuration, and variable update deployment.
- SM client user sessions are logged.
- SM client user actions are not currently logged.
- SM logs all system events.
- SM logs all DyNet messages to/from SM.
- SM logs all messages to/from FIAS (occupant names are removed).

For more information on log files, refer to the Ethernet Gateways Commissioning Guide.

9 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.

More details about standards are available in the General Security Statement under Signify Security: selected best practices > governance, education, and training:

https://www.signify.com/global/security-and-privacy- statement-for-connected-products

10 Shared responsibility

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.
For example, in projects where integration with a separate third-party system requires use of an unsecure communication protocol such as FIAS, a secure VPN tunnel may be used. This minimizes exposure of the unsecure protocol but does not provide full end-to-end encryption.

These are the typical shared responsibilities with the customer:

- Securing the installation, hardening and use of the SM server.
- Integration with third-party systems, such as property management systems or building management systems.
- Implementation of industry protocols such as FIAS, 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 password changes.

10.1 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.

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

10.2 Security maintenance activities

All valid licenses for 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 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.

10.3 Security advisory

This table lists the potential vulnerabilities that we consider to be the responsibility of the customer.

Area of Concern	Responsibilities
1. Attacker can read/modify device configuration and clone an RS-485 field device.	Restrict access to the RS-485 field network. Gateways and controllers must be installed in a secure electrical enclosure. All wiring should be hidden and physically protected from unauthorized access.
2. DyNet IP field network is accessed to attack shared IP network resources.	Customer's responsibility to use either separate VLANs or physically separate cabling from other Ethernet provided services. Ensure gateways are in a secure room, physically accessible by only authorized persons.
3. Attacker can attack the control network for a long time undetected.	Create system logging capabilities for SM integrated into the Customer's IT monitoring functions (such as IT SIEM or IDS or IPS).
4. Unsecured connections from SM to integrated systems (e.g. OPC, PMS, HVAC)	Customer's responsibility to secure the connections to integrated systems.
5. User accounts may be subject to a brute-force attack if using basic authentication and users employ weak passwords.	Customer's responsibility to guard the security of the corporate accounts. Recommend implementing LDAP if password policy enforcement is required and to use complex passwords (e.g. 8-12 characters).
6. SM Server (database) accounts may be compromised.	Customer's responsibility to prevent unauthorized access and brute force attacks
7. SM is accidentally exposed and accessed via remote connections.	Customer's responsibility to harden SM server OS. Customer's responsibility to prevent unauthorized remote connections.
8. A single insider (employee or otherwise legitimate user) can change configurations and see system data outside of normal access rules and/or conditions.	Customer's responsibility to manage users.
9. Attacker accesses another user account and cannot be tracked for access and changes.	Customer's responsibility to maintain session logs and have users lock terminal and use screen savers that lock out users after a short timeout period.
10. The SM server software applications have no protection from malicious code, tampering, or reverse engineering.	Customer's responsibility to guard the security of the server, including running antivirus software.
11. No application level security audit. Attacker can alter event/audit logging.	Customer's responsibility to configure LDAP if it is required to log login attempts. Ensure that audit logs are read only and properly backed up.
12. SM cannot be accessed anymore due to a DOS attack.	DOS protection is customer's responsibility.
13. A single insider gains access to the site private key and uses it to decrypt control system communications over the IP network.	Customer's responsibility to securely store the site private key that is used to sign certificates for Ethernet enabled devices.

11 Reporting security incidents

Security incidents for Philips Dynalite systems are to be reported via the Customer Satisfaction team of the market region. Vulnerabilities in the software or physical devices' firmware are to be reported via the coordinated vulnerability disclosure web page:

https://www.signify.com/global/vulnerability-disclosure

12 Legal Disclaimer

This information is provided for informational purposes only. It represents the current product information as of the publication date. These are subject to change without notice.

Customers are responsible for making their own independent assessment of Signify products or services and the use thereof. This information is provided "as is" without warranty of any kind, whether express or implied. This information does not create any warranties, representations, contractual commitments, conditions, or assurances from Signify, its affiliates, suppliers, or licensors. The responsibilities and liabilities of Signify and its customers are defined in the agreements between Signify and its customers. This information is not part of, nor does it modify, any agreement between Signify and its customers.

R04, 22 June 2022

Philips Dynalite

www.lighting.philips.com/dynalite