

Architecture STR

Room centric lighting and building control for hotels, managed residential and healthcare facilities.

Contents

1	Introduction.....	02	9	Secure Installation Requirements (for customers)	17
2	System Architecture and Security	03	9.1	Additional hardening requirements	18
2.1	Overview	03	9.2	Security Configuration options.....	19
2.2	Integration with other systems.....	05	9.3	Instruction and Recommendation for Security Tooling	20
3	Network Security.....	06	9.4	Security Maintenance Activities.....	20
3.1	Trunk Network	07	9.5	Security Mitigation	20
3.2	Floor network	07	10	Security Operations Requirements (for Customers).....	21
3.3	Room network.....	07	10.1	Accounts on server and devices.....	21
3.4	Integrated systems	07	11	Security Maintenance Requirements (for Customers).....	22
3.5	Dashboard.....	08	12	Security Incidents	22
3.6	Third-party apps	08	12.1	How to report a Security Incident.....	22
4	Device and Physical Security	09	13	Coordinated Vulnerability Disclosure.....	23
4.1	Firmware and configuration updates.....	10	13.1	How to report a vulnerability	23
4.2	Decommissioning.....	11	14	Known Vulnerabilities and Security Advisory .	23
4.3	Product replacement	11	15	Legal Disclaimer	23
5	Cloud services.....	11			
6	Data Classification and Inventory.....	11			
7	Compliance to (International) Standards.....	13			
8	Shared Responsibility Model.....	14			
8.1	Responsibilities.....	14			

1 Introduction

As connected lighting systems are an integral part of the Internet-of-Things (IoT), they are also associated with the same security risks as other devices connected to internal networks.

Most companies use well established procedures to reduce the risk of data breaches. Company-issued computers, smartphones, tablets, and so on, are considered attack vectors that must comply with certain rules in order to be trusted and granted access to a corporate network. The same procedures also apply to IoT systems connected to a corporate network.

The key concerns regarding an IoT solution deployed on a corporate IT network are:

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

This document addresses Interact Architecture STR security concerns 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 room devices, as well as user access to the server, browser-based dashboard 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 Architecture STR 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

Architecture STR is an on-premises system based on the modular Philips Dynalite controls architecture.

The system proposition is designed to deliver focused operational benefits to building owners and hospitality operators by enhancing guest experience, increasing staff and operational efficiency, and improving energy management.

Architecture STR systems are implemented with a combination of hardware, software, protocols, integrations, and services that together provide a scalable IoT solution for smart buildings.

2.1 Overview

The system consists of the following building blocks:

Hardware	<ul style="list-style-type: none">• Dedicated Guest Room Management System (GRMS) controllers with system tuned firmware.• Ethernet gateways provide secure connections between the server and the rooms.• Expansion via the full Dynalite portfolio of controls products.• Tailored sensors and user interface panels to meet occupant needs.
Software	<ul style="list-style-type: none">• On-premises software with dedicated architecture for a highly scalable 'room centric' system.• Realtime visibility via the multiroom dashboard.• Expanded connectivity with API's.
Services	<ul style="list-style-type: none">• Control and/or monitoring of room services such as, lighting, occupancy, drapery, temperature, fans, wakeup alarms, doors, windows etc.• Defined system architecture with templates to achieve fast, consistent, brand compliant projects.• Factory pre-programming and remote bulk update features for lifecycle management.
Ecosystem	<ul style="list-style-type: none">• Certified integrations with property management, access control, housekeeping and other operational hospitality systems.• Cross promotion and specification to drive interest in the system.

Multiroom System Manager server software manages the system databases and integrates with other building systems via software gateways. APIs enable secure access to the multiroom dashboard and third-party interfaces.

Control devices connect via trunk-and-spur topologies and communicate using the DyNet protocol. System Manager server and the PDDEG-S floor (Ethernet) gateways connect to the Ethernet trunk network. Gateways are typically installed in the server room. They connect to the DDRC-GRMS-E controllers in each room and manage traffic between the trunk and spur IP networks.

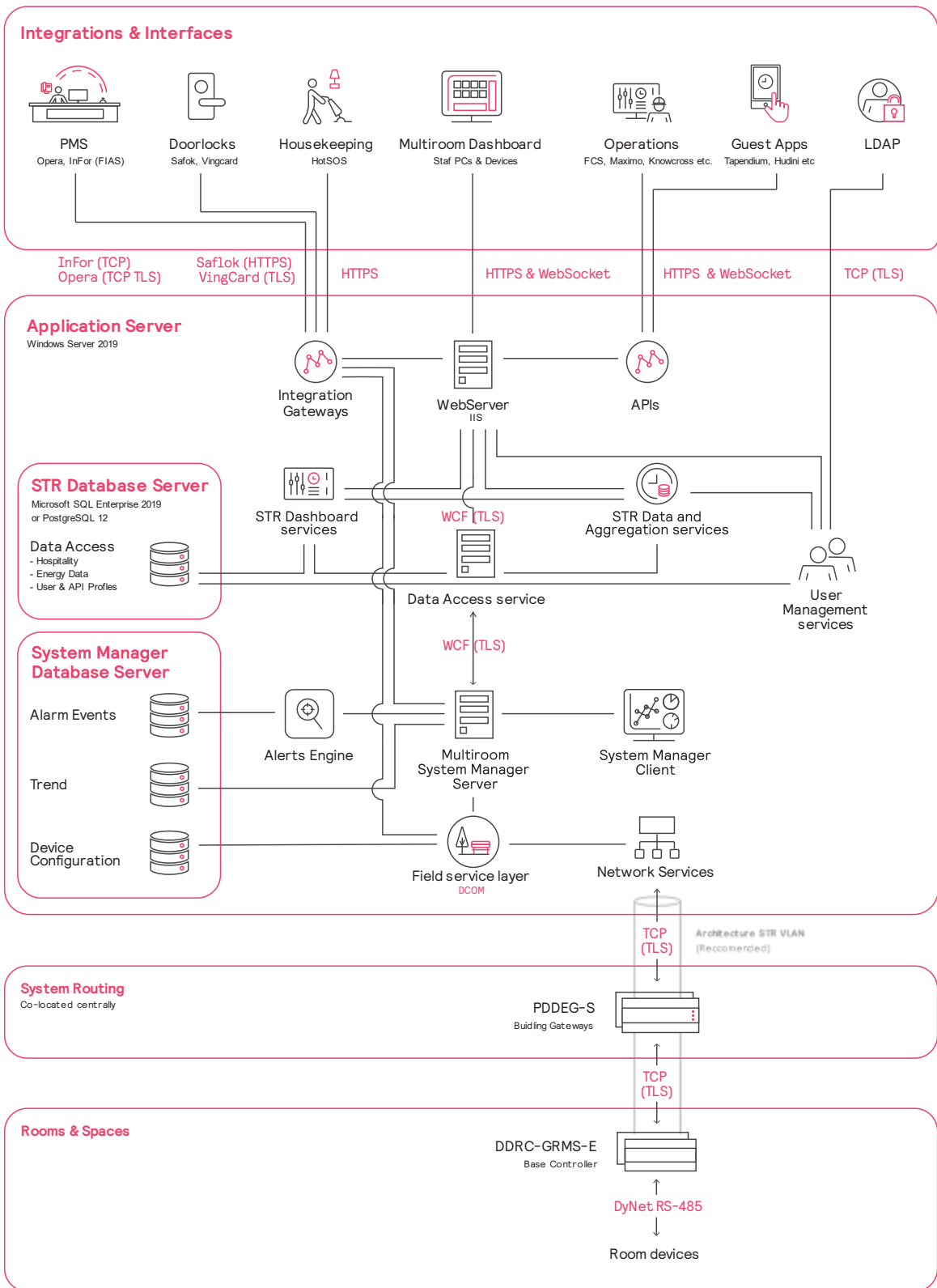
Room devices such as load controllers, user interfaces, sensors and integration devices form an RS-485 field network installed in each room. The system uses distributed intelligence, so devices operate independently of the System Manager head-end software.

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.

A cohesive software suite is available for Certified Systems Integrators (CSI) to design, build, configure, control, monitor and manage the lighting control system with customizable templates to help fast-track common system settings. In addition, the software provides 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.

Architecture overview



There are several focus areas in architecture STR that are comprehensively secured:

1. **Firewall Protected Rooms**

A network firewall in each room controller prevents intruders from being able to control or intercept traffic from one room to another, or from anywhere else in the property. Sitting between the room controllers' room-network and building-network ports, the firewall blocks on a firmware level, any attempt to pass access or configuration commands out to other rooms or to the system on behalf of other rooms.

In addition, an IP connection to the control system is closed to any user without a matching encryption certificate. This prevents remote configuration or resets being attempted to local room devices from the IP network.

2. **Building Network Encryption**

All traffic travelling from the room to the server is encrypted to prevent interception or unwanted injection of messages. Interact software uses only NIST-approved encryption algorithms, ensuring that only strong cryptographic algorithms are implemented.

Using Transport Layer Security (TLS 1.2 or later), network traffic such as room statuses, sensor measurements or control messages are encrypted. Hardware acceleration in the controller for encryption ensures that there is no cost to critical real-time data.

The architecture uses a client/server relationship from server to floor gateway and from room controller to floor gateway, ensuring that trusted links are only being initiated from valid devices. Certificates within devices are encrypted.

Combining network encryption and room controller firewalls, provides comprehensive protection against system intrusion.

3. **Secure Interfaces**

Architecture STR APIs use HTTPS for the dashboard and third-party interfaces.

When providing hospitality team members with dashboard access, the administrator assigns a user profile to give that employee only the required level of access. This limits the functions and floors they can access. For easy and secure login and password management, Active Directory can provide user authentication before passing the user to match their profile for dashboard permissions.

For third party interfaces/systems connecting via our API, these are considered 'Integration users'. The administrator sets up the credentials and access permissions and provides a Client ID and Client Secret to the integrator. Once approved, data transfer is over an encrypted connection to ensure data always remains secure.

From the secure server room, the following enterprise clients can be run on the server, SM Configuration and Data Access Configuration. The SM Client is installed on the server and can be installed on user PCs but is not supported for STR.

4. **Secure Databases**

System Manager uses PostgreSQL as the default database manager. However, customers can choose to use Microsoft SQL Server for all databases. Microsoft SQL Server 2019 Standard or Enterprise Edition supports encrypted databases with Transparent Database Encryption (TDE).

2.2 **Integration with other systems**

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

Integrations

- Software gateway integrations using standard industry and proprietary interfaces and protocols, such as APIs, LDAPS, SMTP.
- 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.

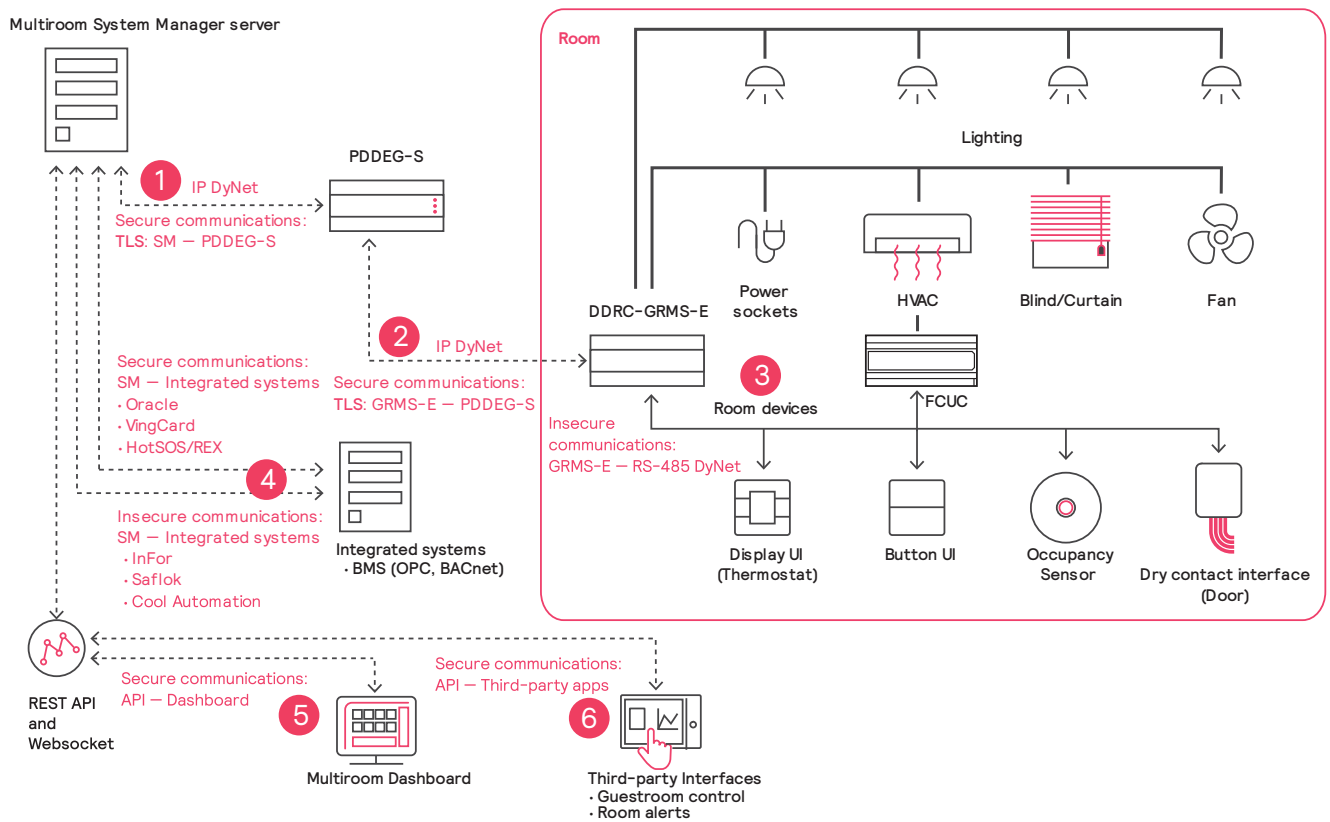
3 Network Security

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

The network architecture is split in six security groups, as follows:

1. SM to PDDEG-S (Trunk network).
2. PDDEG-S to DDRC-GRMS-E (Floor network).
3. DDRC-GRMS-E to RS-485 DyNet Devices (Room network).
4. SM to Integrated systems*.
5. SM API & Websocket to Dashboard.
6. SM API & Websocket to third-party interfaces.

System Connections



- ☰ *Specific integrated systems may be secured with TLS encryption.
- ☰ More information about network architecture and integration can be found in the Architecture STR IT Guide.

3.1 Trunk Network

Client/Server – SM connects as a client over TCP TLS to a known whitelist of PDDEG-S gateways. This means intruders on the IP network cannot connect as a client to SM.

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

3.2 Floor network

PDDEG-S Floor (Ethernet) gateways connect securely over Ethernet to System Manager and to DDRC-GRMS-E room controllers in each room.

Client/Server – DDRC-GRMS-E connects as a client over TCP TLS to a known whitelist of PDDEG-S. This means intruders on the IP network cannot connect as a client to DDRC-GRMS-E.

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

3.3 Room network

Room devices such as load controllers, user interfaces, sensors and integrated devices form an RS-485 sub-network which is managed by the DDRC-GRMS-E room controller. Room controllers have flexible outputs for lighting, power sockets, air conditioning, drapery, fans etc.

RS-485 DyNet is not secured. Cables are made as physically inaccessible as possible. Due to the DDRC-GRMS-E inbuilt firewall, a rogue guest cannot attack the building or other rooms from the RS-485 network in the room.

3.4 Integrated systems

System integration facilitates two-way communication for unified, sitewide intelligence with third-party network systems to exchange commands and data about the site's operation. Popular hotel systems are seamlessly integrated with Architecture STR using a relevant gateway device or multiroom 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 hospitality systems is via common industry protocols that often do not provide secure alternatives. Therefore, alternative mitigating controls should be implemented. User access to these systems is the responsibility of the Hotel operator.

The following Integrations are available:

- PMS (FIAS protocol)
 - Oracle Hospitality*
 - InFor
- BMS/HVAC
 - CoolMaster
 - BACnet
 - OPC
- Access Control
 - Dorma Kaba – Saflok
 - ASSA ABLOY – VingCard*
- Housekeeping
 - HotSOS/REX**
 - FCS – eHousekeeping & Connect (API)**
- Ecosystem
 - Tablets/Apps (API)**
 - SMTP/Email Server*
 - LDAP using LDAPS or StartTLS*

* Secured with TLS encryption.

** Secured with HTTPS encryption.

3.5 Dashboard

Requests from the dashboard web app to the dashboard APIs are always HTTPS. HTTP is not supported. Realtime update events sent from the IIS webserver to the dashboard web app are over WebSocket Secure (WSS).

Authentication at dashboard login is by username/pw which can either be managed in the application or can be integrated with Microsoft Active Directory. Cookies are encrypted.

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

3.6 Third-party apps

Encrypted bearer tokens provide authentication when making API requests and when connecting to the websocket. The third-party client requires a valid token to connect to the secure websocket. The client must authenticate with the usermgmt API to get issued the token.

Requests from third-party apps to the multiroom APIs are always HTTPS. HTTP is not supported. Realtime update events sent from the IIS webserver to third-party apps are over WebSocket Secure (WSS). The third-party client is only sent event types permitted in their user profile.

4 Device and Physical Security

This section describes the customer's responsibility to protect the system, by prohibiting physical access to the Ethernet and RS-485 networks, System Manager server, Ethernet gateway devices and RS-485 field network devices.

Multiroom System Manager Server

It is advised that the Multiroom System Manager Server is placed in a secure IT room to which physical access is monitored and restricted only to authorized individuals. Although databases can be installed on a remote machine, from a security perspective, it is recommended to install all active servers and databases on the same machine.

Floor Ethernet Gateways

The PDDEG-S Floor Ethernet Gateways must be physically inaccessible to prevent security breaches. They must be placed in an IT/utility cabinet to limit physical access only to authorized individuals.

The PDDEG-S provides gateway services between the DDRC-GRMS-E room controllers and the System Manager server. It uses a TLS certificate to establish secure network connections.

PDDEG-S Ethernet gateways feature the following security measures:

- Webserver is disabled for Architecture STR systems
- Minimization of externally available services
- Only signed secure firmware updates are deployed
- Secure bootloader
- Default secure port numbers
- Encrypted IP communications

The QR code sticker on the PDDEG-S 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 (must be changed upon installation)

Room Controllers

The room controller connects the RS-485 room sub-network and the IP floor network. It also has its own lighting control outputs. Although physical access to the lighting control devices cannot be excluded, following the system installation guide and the associated Installation instructions for each lighting control device, mitigates risk of tampering by unauthorized individuals. Room controllers, load controllers and lamp drivers must be installed in an approved enclosure with access restricted to facility management and electrical installers.

To maximize system security, the control cabling for the field network such as Ethernet, RS-485 DyNet, DALI and DMX512 buses must be hidden to restrict physical access (for example, concealed in the wall or ceiling space and requiring tools to gain access).

The device features the following security measures:

- No hardware debug interfaces available
- Port security
- Encrypted IP communications
- Secure firmware update via signed updates
- Hardened Operating System
- Minimization of externally available services
- No user login possible; only device to device communication

Room devices

It is recommended to restrict physical access to the room devices, by placing them in a secure electrical enclosure or in the ceiling or wall for sensors and user interfaces.

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 system installation guide and the associated Installation instructions for each lighting control device mitigates the risk of tampering by unauthorized individuals.

Physical access to the lights, user interfaces, dry contact inputs and sensors can't be prevented by Signify as they are attached to the walls and ceiling in the room, thus falling under shared responsibility.

Load controllers, sensors, drivers, and switches are devices that measure, receive and send data within the lighting network. The 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*.
- RS-485 sub-networks are firewalled by the DDRC-GRMS-E room controllers.

🚫 Unauthorized access to an RS-485 room network or room devices only impacts that one room.

📄 The list of current devices can be found in the Architecture STR System Guide.

4.1 Firmware and configuration updates

Firmware updates for on-site devices are updated on-demand when there is a new firmware version. To ensure continued security, all gateways and room devices receive the latest firmware updates, in terms of both security and features.

System Manager server is always connected to control network devices, which facilitates an efficient update mechanism. For example, if a new feature requires a new software version to enable functionality, then the firmware will be updated as well. This way, the system and firmware are always up to date with each other, and the latest features and security updates are deployed together.

Device firmware and configuration for templated devices can be updated from System Builder by opening the SM Config database and starting a new system deployment per room profile.

- A firmware update deployment starts with a System Builder secure signed and encrypted firmware file which is then deployed by System Manager to all selected devices in the deployment. Non-templated device firmware can be updated individually from System Builder.
- A configuration update deployment starts with a modified System Builder device configuration within a room template, which is then deployed by System Manager to all selected devices in the deployment. Non-templated device configuration can be updated individually from System Builder.

4.2 Decommissioning

This section explains the decommissioning of Ethernet Gateway and GRMS-E Room Controller devices. These devices store unique site credentials, such as user account information, security certificates and IP addresses.

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

- The factory reset mechanism for the floor gateway 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 room controller requires System Builder to perform a Device Factory Reset with the delete Certificate and delete IP address checkboxes selected. The device can then be disconnected from its power supply.

When removing the product from its intended environment it is recommended to delete security certificates, configuration data and log files stored in the product; and securely dispose of the product to prevent potential disclosure of data contained in the product that could not be removed as described in above.



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

4.3 Product replacement

PDDEG-S – Create and upload a site device certificate and copy configuration data from the previous device to replacement devices. Then replace the device in Config DB.

Room controller – Create and upload a site device certificate or confirm the spare device already has a certificate. Setting the same DIP switches on a replacement room controller, enables it to function identically to the failed room controller. It is recommended spare room controllers be kept in a secure location.

Multiconfiguration Antumbra – setting the same DIP switches on a replacement multiconfiguration Antumbra, enables it to function identically to the failed Antumbra. It is recommended spare Antumbra user interfaces be kept in a secure location.

Room controller and room devices are templated in each room profile. Firmware and configuration for replacement devices is updated via the room profile deployments feature. Non-templated devices are reprogrammed by loading their configuration from Config DB and saving to the device.

5 Cloud services

Not Applicable

6 Data Classification and Inventory

Hospitality data pertains to usage of the room and its devices by guests and staff. The Architecture STR system does not store or process any personal data. But we do provide state information from the room (as above) that, linked to personally identifiable data (such as guest name), can be considered personal information. If this data is linked by the customer, the customer is responsible for handling the data according to local legislation. The system stores the following data assets.

Data Assets	Description	Classification	Data Location	Processing Time	Retention Time	Retention Category
System credentials	Credentials and identities of services and devices, needed for establishing and maintaining system connectivity. LDAP server account details for Active Directory integration. SMTP server account details for email alerts.	Secret	Config DB User Management DB	customer decision	customer decision	customer decision
User identities and roles	Multiroom dashboard user identities and roles, hashed password (if not using Active Directory integration). Integration account identities and roles, hashed password. SM user identities and roles: authorization levels mapped to Windows user IDs.	Secret	Config DB User Management DB	customer decision	customer decision	customer decision
System and device configuration	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.	Confidential	Config DB User Management DB	customer decision	customer decision	customer decision
System and device status and history	Status and history of the system, including online/offline status of devices, alarms, events, user logon/off (SM users and SM Client users), history of event management.	Confidential	Alarms DB	customer decision	customer decision	customer decision
Guest room activity	Status and history of room usage by the guests and staff: occupancy statuses, DND, MUR, room service and laundry pickup requests, doors (entry, balcony, safe), curtains, wakeup alarm settings, HVAC settings & temp/humidity data, lighting settings. Room events from Multiroom dashboard control and from FIAS.	Confidential	Hospitality Dashboard DB	customer decision	customer decision	customer decision
Energy usage data	Status and history of estimated system energy usage.	Confidential	Energy DB	customer decision	customer decision	customer decision
Application log files	Text logs for SM, DataAccess, IIS Web APIs, deployment logs (firmware, configuration, and variable updates). Text logs on PDDEG-S. Stored on device for up to 28 days before being overwritten. Can be managed and downloaded using System Builder.	Confidential	SM Server PDDEG-S	customer decision	customer decision	customer decision
Network log files	Network log files on SM server for trunk DyNet messages and Fidelio messages to/from FIAS (guest names are removed). Network log files on PDDEG-S for messages sent and received on spur ports. Stored on device for up to 28 days before being overwritten. Can be managed and downloaded using System Builder.	Confidential	SM Server PDDEG-S	customer decision	customer decision	customer decision

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 Architecture STR 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.

Development	Infrastructure	Installation	Operations	Maintenance	Decommiss.
Secure Development SDL	Network Security	Secure Installation	Business Continuity	Application Updates	Secure Data Removal
Encryption and Data Security	Data Center Physical Security	Hardening	Incident Management	OS Updates	
 Customer			Credential Management	Threat and Vuln. Management	

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 FIAS 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
6.2	External License renewal	Operation		R A	C
7	Backups				

	Responsibility for on-premises components	Phase	Signify	Customer/CSI	Third-party
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 when 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 using role-based access control.
4. Secure communications between Ethernet devices.
5. Secure communications to the multiroom dashboard and APIs.

Physical and/or logical separation of the lighting network from other IP networks

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 and cabling

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.

User management using role-based access control.

The Multiroom dashboard user management page is used to control access to the web-based dashboard. Users, user profiles, user permissions, and floor access are configured by users with User Management permissions. Optionally, users can be linked to their corporate LDAP services for user account control. We recommend the use of strong passwords and only assigning minimum permissions required for each user profile.

Secure communications between Ethernet devices

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 site-specific certificate chain.

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 webserver on Ethernet gateways must be disabled during commissioning for all STR projects.

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

Secure communications to the multiroom dashboard and APIs

STR systems use the OpenID standard. Each client installation must be implemented respecting the same security requirements and recommendations as described in OpenID.

Multiroom dashboard web app accounts are created locally in the Multiroom dashboard User Management pages. Accounts can be linked to Active Directory. Administrators with User Management permissions can create and assign profiles for dashboard users. Each dashboard user must have an assigned user profile and each user profile has a set of defined permissions. The administrator can also set a universal inactivity logout period for all users. All accounts with Project Admin or User Management permissions automatically log out after a maximum of 1 hour of inactivity.

Multiroom API integration user accounts are created locally in the Multiroom dashboard Configuration pages. Administrators with Configuration permissions can set credentials for integration users to access the API. Each API client uses a unique Client ID and Client Secret to obtain a temporary authentication token. This token must be refreshed periodically, ensuring that only authorized apps and clients have secure access to permitted API and WebSocket functions.

For Multiroom dashboard users (if not using Active Directory) the password is stored locally and is hashed and salted. For Multiroom API integration clients the password is stored locally and is hashed and salted.

For more information refer to the Multiroom Dashboard User Guide and the Interact Developer Portal:

<https://www.developer.interact-lighting.com>

As part of the handover of the system to the customer, the customer's IT team configures HTTPS access to the dashboard 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. The 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 (Dynamilis 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.dynamilis/>") 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's 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.

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 Interact 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)	443 HTTPS Server	For Hospitality Dashboard and APIs.
	389 LDAP Client.	For secure outbound communication using LDAP or LDAP+StartTLS. An alternative port may be configured.
	636 LDAPs Client.	For secure outbound communication using LDAP over SSL (LDAPS). An alternative port may be configured.
	3270 HTTP Server	For dormakaba Saflok Messenger LENS.
	3389 RDP	For remote desktop connections
	8084 WCF	8084 may be required if using the System Manager Client application to connect to SM server. If SM client is not required to run as a remote client, then this port can be closed in the Windows firewall.
	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	443 HTTPS Server	For secure webpages, firmware upgrades and API.
	50443 TCP TLS Server.	For secure Ethernet spur/ inter-spur connections.
	51443 TCP TLS Server	For secure Ethernet trunk connection.
	5353 IGMP	For mDNS.
	123 NTP Client	Network Time Protocol used to synchronize real time clock from the internet.
PDEG Only used for CoolMasterNet integration	10102 TCP Client	CoolMasterNet Text and Binary integration
	50000 TCP Server	Default port for configuration and firmware updates
	5353 IGMP	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	For mDNS.

- 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

Customer decision.

9.4 Security Maintenance Activities

Interact 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 building management systems or hospitality systems is often implemented via protocols such as BACnet or FIAS. 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 Architecture STR 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:

PostgreSQL Database

- PostgreSQL is the default database for Data Access/Multiroom Dashboard and APIs.
- 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.

Microsoft SQL Server Database

- Microsoft SQL is an alternative to the PostgreSQL database for Data Access/Multiroom Dashboard and APIs.
- Superuser is setup during SM installation to allow access to Microsoft SQL Server or can optionally use Windows Authentication.

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 superuser. SM client isn't required in the system, as it has been replaced by web clients. If for some reason the hotel does install other instances - SM client uses Windows user's accounts to authorize, and role-based permissions can be assigned in the SM Configuration client. Windows users may be configured locally on the SM server or centrally in Active Directory.

Multiroom Dashboard

- Dashboard users with defined permissions.
- Superadmin or any user with User Management permission can access User Management to enable user account permissions (access control) and privileges (user rights) for staff to access the Dashboard.

Integration API

- Superadmin or any user with Configuration permission can access Configuration > Integrations, to enable integration account permissions (access control) and privileges (user rights) for third-party interfaces to access the RESTful API and websocket.
- Integration client with defined permissions.

Ethernet Gateways

- No user accounts exist in Ethernet gateways for Architecture STR.

11 Security Maintenance Requirements (for Customers)

System updates

Site operations 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 only be deployed by an authorized Signify employee or Value-Added Partner (VAP) representative.

Internally, mature software development and release procedures guarantee the high quality of the Interact 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 www.first.org

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

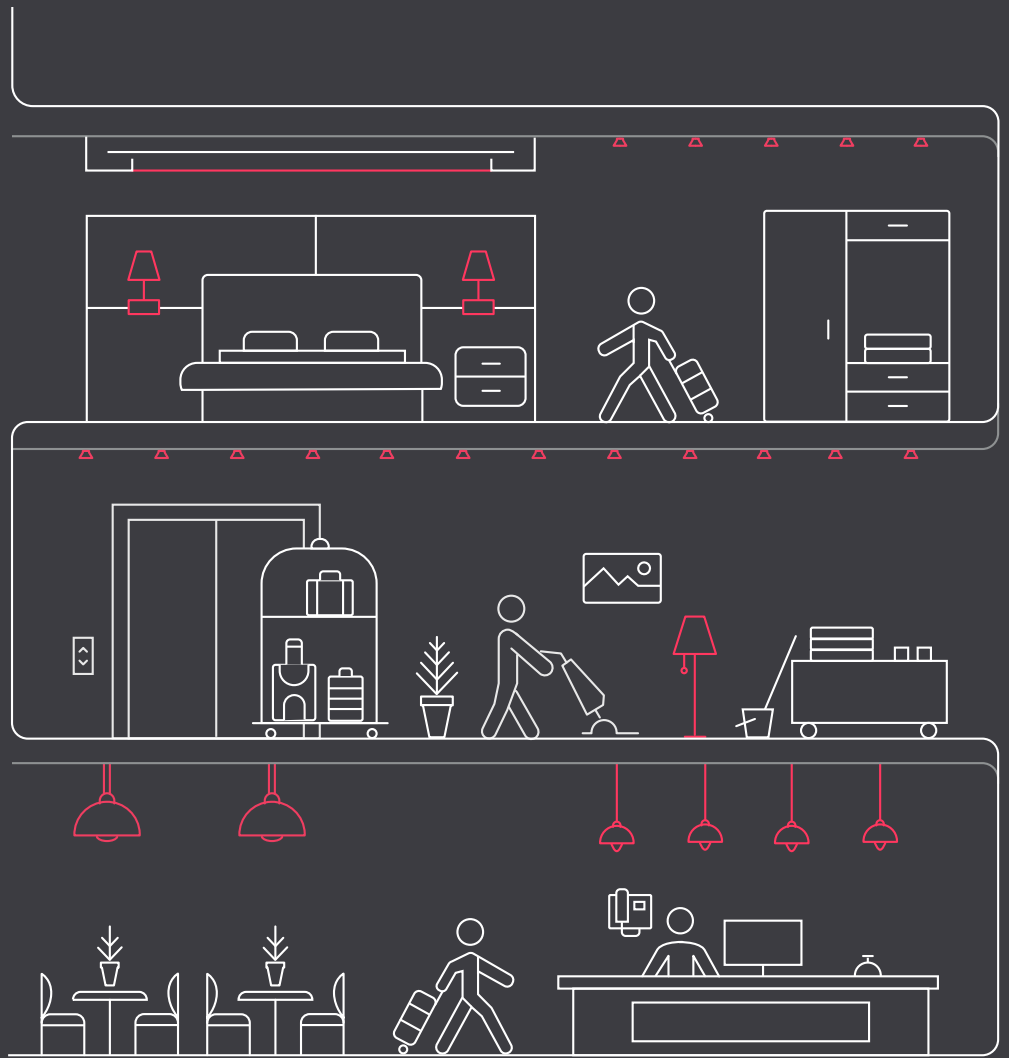
Known vulnerabilities, mitigations and workaround are published on our Security Advisory page:

<https://www.signify.com/global/product-security/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.



Learn more about Interact

www.interact-lighting.com

© 2023 Signify Holding. All rights reserved. Specifications are subject to change without notice. No representation or warranty as to the accuracy or completeness of the information included herein is given and any liability for any action in reliance thereon is disclaimed. Philips and the Philips Shield Emblem are registered trademarks of Koninklijke Philips N.V. All other trademarks are owned by Signify Holding or their respective owners.

Revision 07 – 20th December 2023

interact