interact

Security Statement

Architecture FLX

Multisite - Release 2.1

Contents

1 Introduction

As lighting systems are nowadays an integral part of the Internet-of-Things (IoT), they are also associated with security risks, as with every other device connected to the Internet.

This document addresses security concerns and provides steps to mitigate security issues.

Companies use well established procedures to reduce the risk of corporate data breaches via devices connected to the company's internal network. Company-issued computers, smartphones, tablets, and so on, are considered attack vectors which require to comply with certain rules to be trusted and granted access to an internal corporate network. The same procedures apply for IoT systems that connect to a corporate IT network.

At Signify, the Corporate Security Office manages security governance.

The Product Security Leadership Team, which includes members from the Corporate Product Security organization, business groups, and Product Innovation team, coordinate our security efforts.

A network of security architects and security specialists embedded in the development teams supports security activities related to product development.

All Signify employees are required to attend regular cybersecurity and privacy awareness training. System architects and development engineers must also receive specific additional training and internal security certifications.

Interact software mitigates security risks of a lighting IoT system by employing security strategies that are described later in this document.

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

- Vulnerabilities that result in access to devices or network components on the corporate IT network, such as login credentials, access to servers or storage locations.
- Vulnerabilities that disturb operational performance of individuals or equipment working in a building. It ranges from operating the lights in such a way that it disturbs individuals to fully jamming the network in the building.
- Vulnerabilities in IoT devices that can be used to compromise other services, such as botnets.

1.1 Implementation of security principles

Systems based on the Interact cloud platform are managed by a specialized global operations team. At Signify, we implement a security policy which enforces segregation of duties and least privilege access.

Responsibilities of the team include producing operational specifications and performing maintenance, security updates, vulnerability management, backup, logging, monitoring, and management of events and incidents. The team also performs periodic review of network and application security.

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.

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

More information about the security principles of the onsite Dynalite field devices can be found in the Dynalite Controls Security Statement.

2 System architecture and security

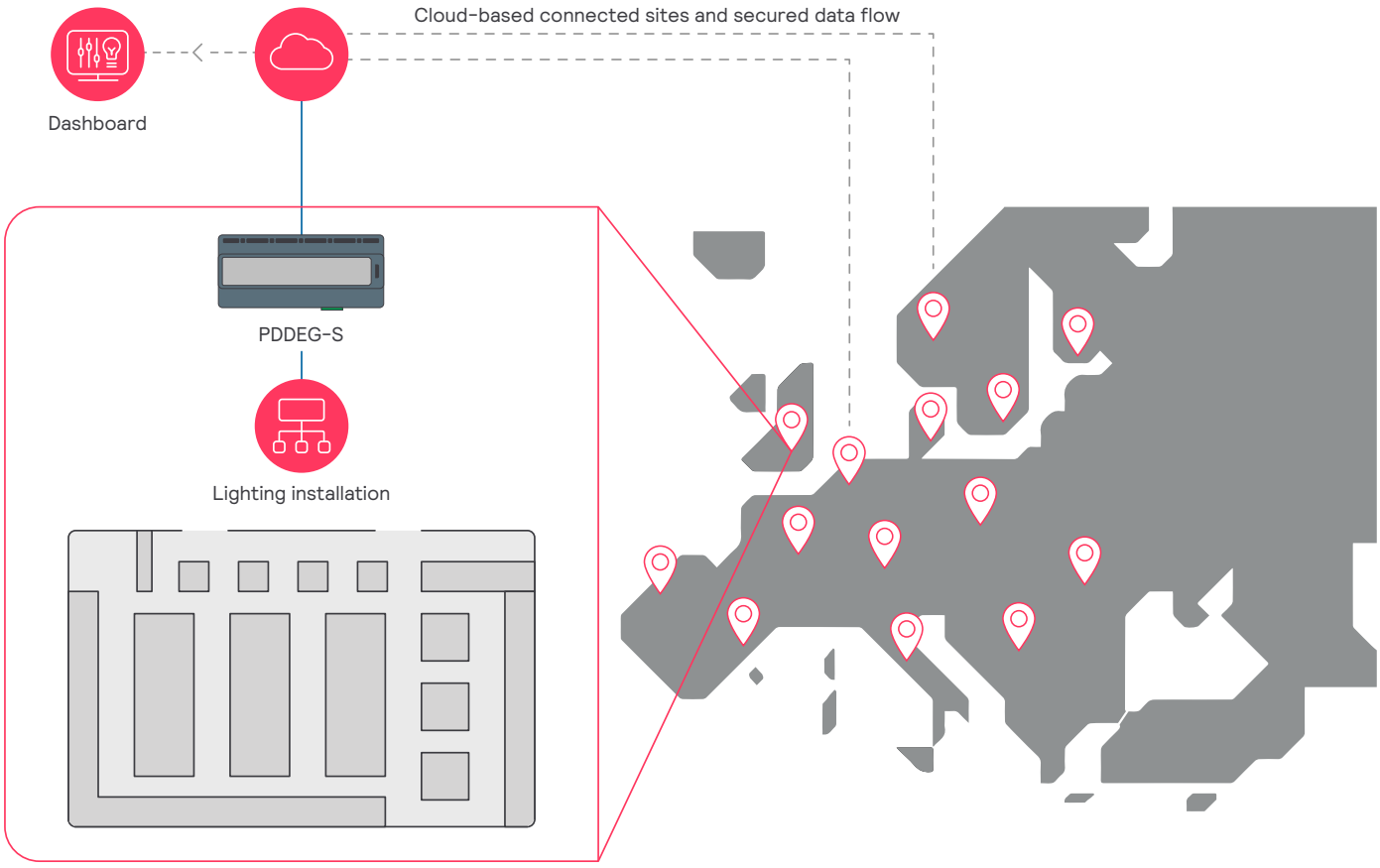


Figure 1 High-level system overview

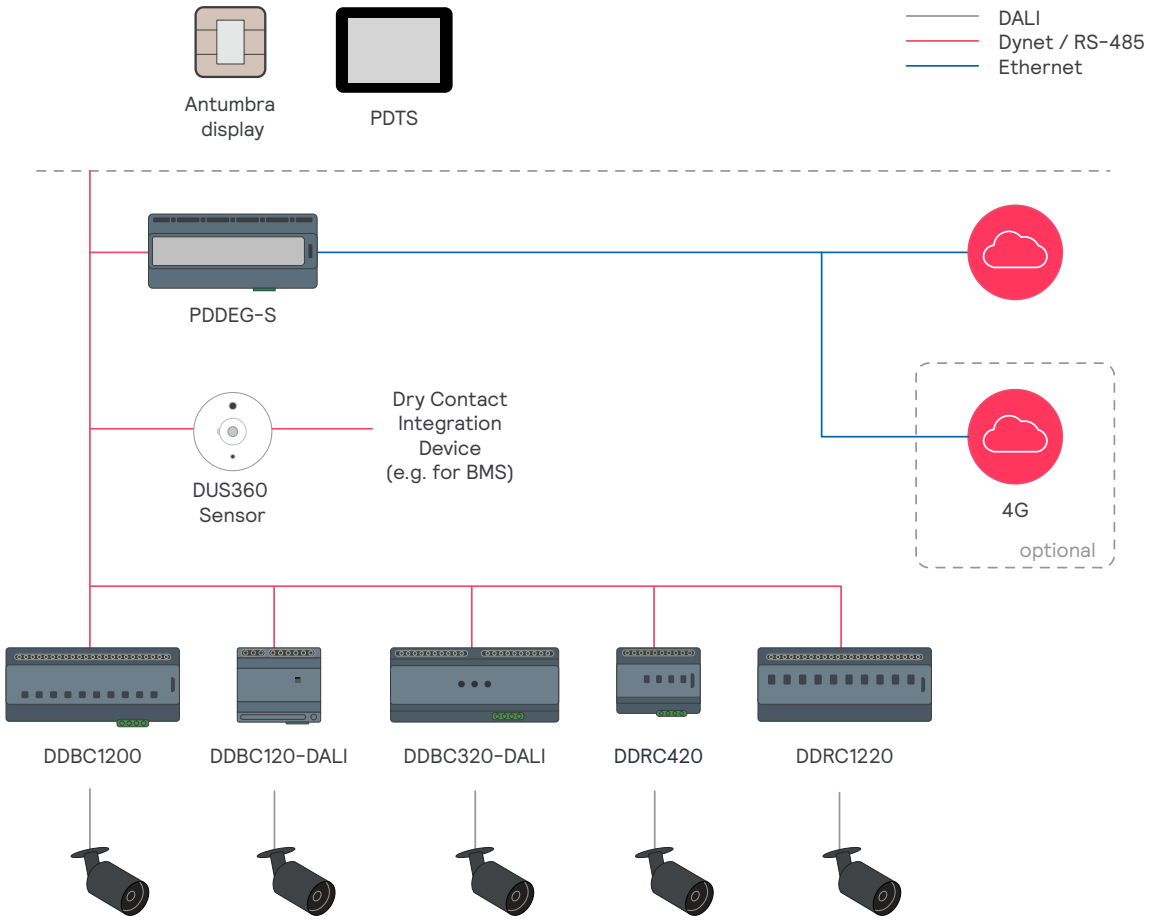
The Multisite system is based on a modular on-premises Philips Dynalite controls architecture with a secure connection to the Interact cloud platform (the cloud), managed by Signify, built on top of it.

The Ethernet Gateway (PDDEG-S) connects securely over the internet to the cloud, and via RS-485 or ethernet to the controllers on site.

The PDDEG-S gateway is a single device that:

- establishes secure connection between the system on-premises and the cloud,
- manages and secures the traffic from the site to the cloud.

The network is connected to services running in the cloud and data collected is also stored remotely in the cloud.



The controllers on-premises are part of a distributed architecture and all have their specific outputs, like DALI, 0-10V, and relay (on/off). The devices such as load controllers, user interfaces, sensors and integrated devices form an RS-485 sub-network which is connected via the PDDEG-S gateway. The devices communicate with each other using the DyNet protocol.

Light control is implemented from the controllers onsite using a DALI network and switchable outputs.

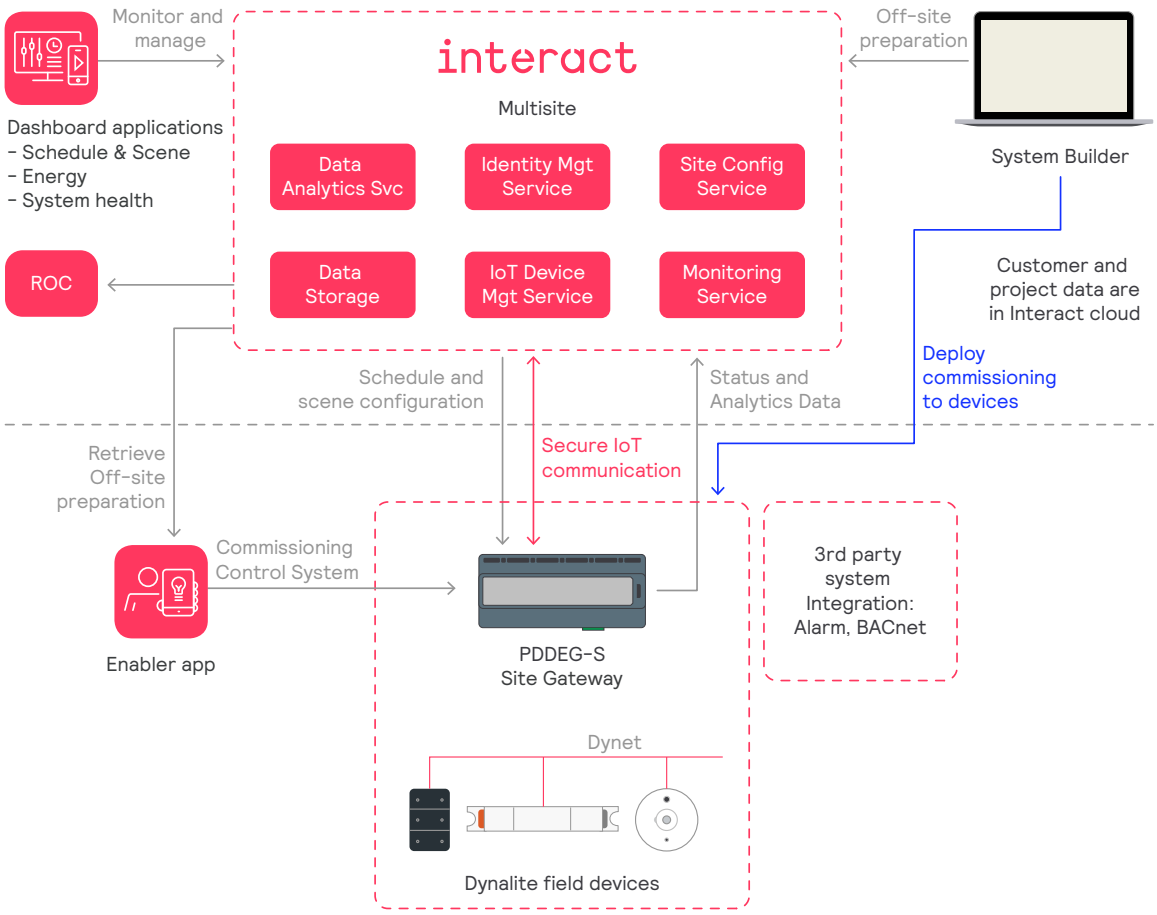
2.1 Integration with other systems

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

Integrations

- Software gateway integrations using standard industry and proprietary interfaces and protocols, such as APIs, LDAPS, SMTP, etcetera.
- Hardware device-based integration such as, 1-10V, DSI, DALI, DMX, Modbus, BACnet, API, etcetera.

3 Network security



This section details how traffic is routed between the access network, customer's network or internet and the cloud platform. The system is connected securely via the internet to the secure Interact cloud platform. This connection can be established via multiple topologies:

- Local network, either delivered by the customer or Signify
- Internet connection via the IT infrastructure of the customer
- Internet connection via the optional connectivity service delivered by Signify

The network topologies are detailed in the *Architecture FLX - Multisite System Guide*.

4 Device and physical security

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

The devices' Operating Systems are hardened by whitelisting of services and libraries that run on them, according to the OWASP IoT framework.

PDDEG-S Ethernet Gateway
The PDDEG-S 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 trunk network. Ethernet Gateways authenticate with Multisite System Manager when they become operational with unique secure user credentials.

The Ethernet Gateway feature the following security measures:
- Webserver access via HTTPS
- Minimization of externally available services
- Only signed secure firmware updates are deployed
- Secure bootloader

Additionally, the PDDEG-S features the following security measures:
- Default secure port numbers
- Encrypted IP communications

The QR code on the PDDEG-S Ethernet Gateway allows easy identification of the device and contains the following information:
- Hardware version of the device
- MAC address
- Serial number
- Default username and password (default password must be changed upon installation)
- 12NC

Load controllers
The controller provides a connection between the wired field network and lighting control outputs. Although physical access to the lighting control devices cannot be entirely prevented, following the 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). Devices feature the following security measures:
- No hardware debug interfaces available
- Encrypted IP communications
- Signed secure firmware updates are deployed (platform specific, some limitations apply)
- Hardened operating system
- Minimization of externally available services
- No user login possible; only device-to-device communication

4.1 Firmware updates

The firmware of on-site devices is regularly updated. From a security standpoint, it is highly recommended that all lighting network devices receive the latest firmware updates, in terms of both security and features.

The Interact cloud platform is remotely connected to the PDDEG-S, which facilitates an efficient update mechanism of this device.

The update heartbeat for network devices might be different than the one of cloud applications, depending on which type of update or what it includes. For example, if a new feature requires a new firmware 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.

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 job or database and saving to selected devices.

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

4.2 Decommissioning

This section explains the details regarding decommissioning of the PDDEG-S gateway and DyNet network control devices.

4.2.1 PDDEG-S Ethernet Gateway

The PDDEG-S can be decommissioned by the operations team. After that the device will no longer be associated with the project and needs to be assigned again before it becomes operational again. Once decommissioned, all operational credentials for the secure cloud connection are removed.

It is also possible to reset the device locally by setting a jumper on the PCB and powering up the device. This will erase all operational credentials and reset the login credentials to the factory credentials. If the device was not decommissioned from the cloud, the device re-registers with the secure cloud platform automatically and gets commissioned again. After this it will be operational again but might require additional configuration actions via System Builder and a concept and schedule deployment.

4.2.2 DyNet network control devices

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

5 Cloud services

Since the lighting system is always connected to the Interact cloud platform, system security is given top priority from the specification phase, also aiming the hardware lifespan of each installation.

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

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

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

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

5.1 Encryption and key management

The Interact software uses only NIST-approved encryption algorithms, which ensures that only strong cryptographic algorithms are used.

In-transit data between the PDDEG-S and the cloud platform is fully encrypted using TLS 1.2 with the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

5.2 Business continuity

Multisite is offered as Software-as-a-Service (SaaS), which is at the core of the Interact business model.

Its services are stored in multiple locations. Backups and other data are stored in various availability zones, in accordance with data jurisdiction requirements to maintain a high level of business continuity.

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

Multisite delivers overall system security by conducting strict operational and account management processes.

Monitoring the traffic and identifying threat situations that belong to regular operational processes are further key processes.

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

5.3 Authentication and authorization

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

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

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

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

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

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

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

5.4 System updates

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

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

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

6 Data classification and Inventory

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

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

The system collects the following data:

Data Assets	Description	Classification	Data Location(s)	Data retention
Job file	Configuration data of devices and sites (including floorplans, background images)	Secret	EU	3 months after ending Software Service
Monitoring data	Status of the system, including online/offline status of sites and devices, alarms, metrics (energy, motion), software-status of devices	Confidential	EU	Deleted upon request of the customer
Customer Site data	Customer meta data (contact details, site locations, etc.)	Internal	EU	Deleted upon request of the customer
User identities and roles	User login data, contact info, roles, and responsibilities	Confidential	EU	Deleted in event of invalid email address
				Deleted upon ending Software Service
Multisite control data	Data control by the system and deployed to the sites. (Schedule control, preset control, change management logging, etc.)	Confidential	EU	Deleted upon request of the customer
System credentials	Credentials and identities of services and devices, needed for establishing and maintaining system connectivity	Secret	EU	3 months after ending Software Service
Device configuration	Configuration for device behavior, also controls some security features like enabling and disabling ports and features; on some devices, this data can contain usernames and passwords	Secret	EU	3 months after ending Software Service
Syslog files	Containing detailed information on device behavior, used for diagnostics	Internal	Local devices / EU	
Amplitude diagnostic data	Containing information on the use of the mobile app; data is anonymized	Internal	EU	
Network log files	Containing detailed information of traffic on the DyNet network. This data is used in analytics determining system state	Confidential	Local devices / EU	

7 Compliance to (International) Standards

Signify is awarded by DEKRA Certification with the IEC62443-4-1 cyber security certification for our connected lighting development process (IEC 62443-4-1). 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 ensuring that all identified security requirements are implemented, verified, tested, and documented with traceability.

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, the IEC 62443 standards, and the ISO/IEC 27000 series.

In terms of data protection of storage and privacy, Signify complies with GDPR.

See the General Product Security Statement for more information.

8 Shared Responsibility Model

The Shared Responsibility Model aims to secure the installation and use of the cloud platform.

See the General Product Security Statement for more information.

A typical Signify System has both on-premises components and cloud components (see Figure 2).

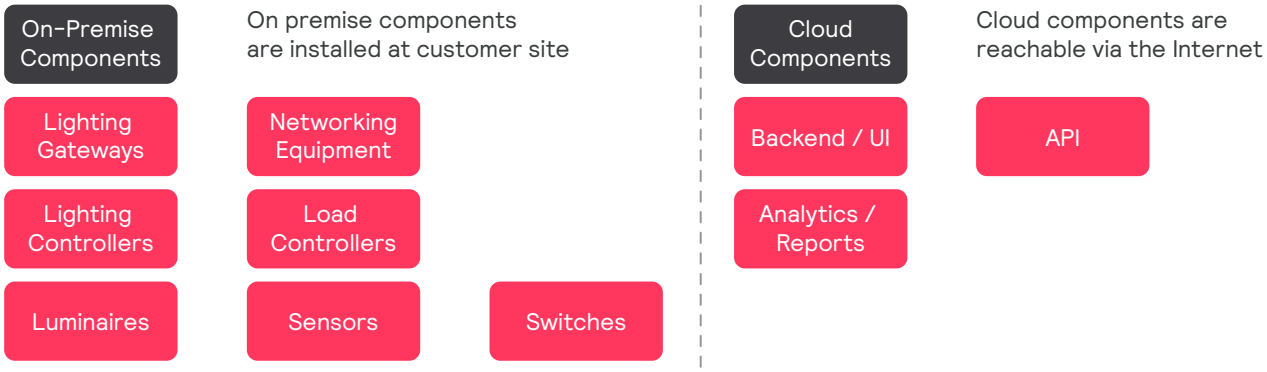


Figure 2: On-premises and cloud components in a typical Signify System

Responsibility for security is typically shared between the manufacturer (Signify) and the customer (see Figure 3 and Figure 4).

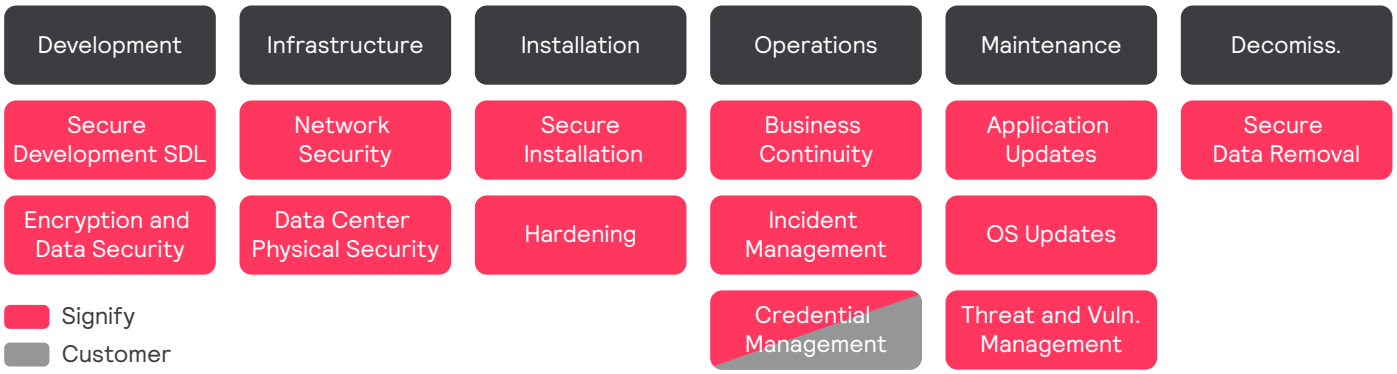


Figure 3: Responsibility for Cloud-components

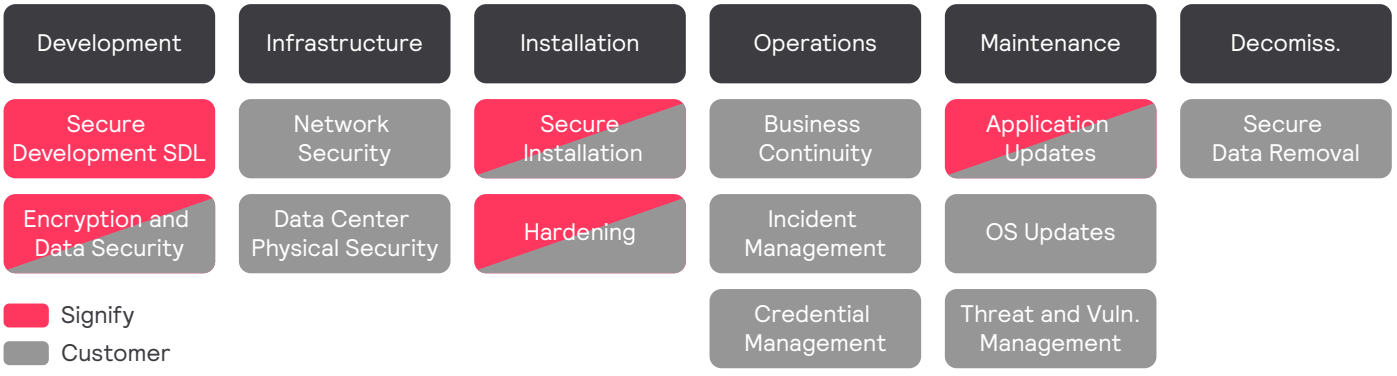


Figure 4: Responsibility for on-premises components

8.1 Responsibilities

Shared responsibility is regulated on a project basis with every customer via legal contracts. It typically covers the following:

- Integration with third-party systems, such as industrial controls, SCADA or building management systems
- Implementation of protocols such as BACnet
- Maintenance of network components
- Physical security of network components, such as placement of the PDDEG-S in a lockable IT cabinet
- Physical security of the Dynalite controller components, part of the lighting network, such as placing them in a lockable cabinet
- Access security policies such as password change
- Other specific responsibilities

Measures to mitigate security risks are also taken on a project basis, depending on the requirements. For example, in such projects where integration with a separate third-party system requires use of an unsecure communication protocol such as BACnet, a secure VPN tunnel may be used. This minimizes the exposure of the unsecure protocol but does not provide full end-to-end encryption.

The data below is for reference only as well as the responsibilities. Each system may have different requirements and activities.

		Phase	Signify	Solution integrator *	End-user
1	**User Credentials Management**				
1.1	Request new account			A	R A
1.2	Approve request				R A
1.3	Create new accounts	Operation	R		A
1.4	Update accounts	Operation	R		A
1.5	Delete accounts	Operation	R		A
1.6	Authorization (roles and sites)		R	A	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 (cloud + gateway)	Operation	R A		
4.2	Update/Upgrade (on premise light control)	Operation		R	A
4.3	Configuration	Installation		R	A
5	**Infrastructure / OS Management**				
5.1	IT installation	Installation		R	A
5.2	Gateway hardening	Installation	R A		
5.3	Patching / Maintenance IT installation	Operation		R	A

		Phase	Signify	Solution integrator *	End-user
6	**Licensing**				
6.1	License renewal request	Operation		I	R A
6.2	License renewal		R A		
7	**Backups**				
7.1	Backup Procedure	Installation	R	R A	
7.2	Configuration / Data Backup	Operation	R	R A	
8	**System Development**				
8.1	Hardening	Development	R A		
9	**Network**				
9.1	Router Configuration (customer IT)	Installation		R	A
9.2	Signify connectivity solution	Operation	R		A
9.3	Update (customer IT)	Maintenance		R	R A
9.4	Patching (customer IT)	Maintenance		R	R A
10	**Monitoring**				
10.1	Scanning for intrusion/malware	Operation	R A		R A
10.2	Performance monitoring (availability)	Operation	R A		R A
11	**Incident Management**				
11.1	Report			R	R A
12	**End Point Protection**				
12.1	Web application firewall	Operation	R A		
12.2	Site IT firewall	Operation		R	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.

* With Solution integrator is meant the party who integrates the solution at the site of the customer. This can be either personnel from Signify or from a third party (for example a CSI).

9 Secure installation requirements (for customers)

Securing the system at all points of connection is critical to installing technology across the building.

To mitigate risks, it is recommended to implement the following security measures:

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

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

Restricted physical access to control network devices
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 undergo a check for before being installed by the electrical contractor.

User management tools using role-based access control.
The Multisite System Manager dashboard requires user authorization, which is configured by the super administrator user who adds Users, roles, permissions, and tenancy access. When using a domain, Windows users can be linked to their employer's corporate LDAP services for user account control. We recommend the use of strong passwords.

Secure communications
The PDDEG-S Ethernet gateway and Ethernet enabled load controllers must have a security certificate installed to securely connect to each other and to Multisite System Manager via the IP network and without internet connectivity.

In-transit data between the Multisite System Manager dashboard and the PDDEG-S Ethernet gateway is fully encrypted over a TCP TLS connection. The TLS connection is established using a device specific certificate and private key.

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

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

For commissioning the following ports are open:

- Port 443, secure, required to configure the device
- Port 52145 (IPv6, UDP), needs to be closed by the commissioning engineer after discovery of the PDDEG-S
- Other ports (secure/non-secure) can be opened by the commissioning engineer, but this is not in line with the requirements laid down in the Commissioning Guide.

Important
Follow the instructions in the Architecture FLX - Multisite Commissioning Guide to close port 52145.

9.1 Additional hardening requirements

Not applicable

9.2 Security Configuration options

All components having established secure practices to protect the security certificates and uses 2048-bit RSA keys and AES-128-bit keys for authenticating and encrypting network traffic:

- traffic between the site and cloud
- traffic between the browser of the user and the cloud]

All lighting devices are connected to a lighting network and use DyNet/RS-485, and ethernet.

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, additional services do not need to be publicly available as an attacker might be able to abuse potential vulnerabilities in the services provided to gain access to the system. Therefore, it is advised that security is hardened on the PDDEG-S gateway, which runs Multisite software, or on the IT network it is connected to, to minimize attack surface and vectors. An overview of open ports that are needed for the proper functioning of the system is listed below:

Device	Port & Protocol
PDDEG-S	• 53 DNS (outbound only) • 123 NTP (outbound only) • 443 HTTPS (outbound only) • 5671 AMQP (outbound only) • 8883 MQTT (outbound only)
Interact cloud connectivity	• NTP enabled • DHCP server provided • MDNS discovery enabled • DNS service access available • No proxy • No 802.1x network access control

See Appendix A Endpoints for an overview of all endpoints.

Note

For information regarding the specific outcomes of the Pen test, please refer to the latest TPM report from CompuTest.

Important

It's the responsibility of the customer to configure the port of their IT switch that is exposed to our system interface (PDDEG-S gateway) to the speed of 100 Mbps/Full duplex. It's not allowed to leave it to auto-negotiation, or manually fix it to 1 Gbps. It's mandatory to use these settings to make sure that the system operates properly, with stable gateway connectivity to the cloud and receiving periodical firmware updates.

9.3 Instruction and Recommendation for Security Tooling

Not applicable

9.4 Security Maintenance Activities

Multisite System Manager includes:

- Frequent software releases ensure that vulnerabilities are addressed in a timely manner.
- Firmware updates of the PDDEG-S are provided over the air regularly throughout the licensed period and automatically deployed to the impacted devices.
- For other devices, firmware updates are provided regularly throughout the licensed period. Updates are customer installed unless otherwise included in a lifecycle package.

9.5 Security Mitigation

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

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

10 Security Operations Requirements (for customers)

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

10.1 Accounts on devices or cloud

User account permissions (access control) and privileges (user rights) are needed to use the Multisite System Manager, including, but not limited to operating system accounts, control system accounts and database accounts.

When using a domain, Windows users can be linked to their employer's corporate LDAP services for user account control. Usage of strong passwords is recommended.

11 Security Maintenance Requirements (for customers)

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

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

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

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

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.

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.

12.2 How Signify will manage Incidents

Confirmed incidents (e.g., breach to 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 Personally Identifiable data.

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

See the General Product Security Statement for more information.

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.

Find the Common Vulnerability Scoring System Version 3.1 Calculator.

Security vulnerabilities are handled within our SDL lifecycle, and we share with the customer through our Security Advisory Page. Security vulnerabilities in our clouds are analyzed and patched according to our policy which is the following:

Our processes recommend fixing vulnerabilities identified according to the following timetable:

Severity	CVSS	Timeframe suggested	Comment
Critical	CVSS > 9.0	Immediately	A security advisory will be published and Signify will start development of a solution. As soon as the solution is available, it will be published on the updated advisory
High	7.0 < CVSS < 9.0	1 month	
Medium	4.0 < CVSS < 7.0	4 months	
Low	CVSS < 4.0	Next Major release	

High and Critical vulnerabilities are always fixed within the time frame identified. Medium and low vulnerabilities are addressed in the context of the full system and a fix may get rescheduled depending on more urgent tasks.

Include link to Security Advisory" web page for the product which describes issues and patches applied or requirements from users to take care and apply certain patches (in case of on-premises installation) or firmware updates requirements.

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

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 the use thereof. Any commitments or liabilities in respect hereof are defined in the agreements between Signify and its customers.

Appendix A Endpoints

Endpoint	Port	Transport	Application
8.8.8.8 (see note)	53	TCP	DNS
8.8.8.8	53	UDP	DNS
pool.ntp.org	123	UDP	NTP
0.pool.ntp.org	123	UDP	NTP
1.pool.ntp.org	123	UDP	NTP
2.pool.ntp.org	123	UDP	NTP
3.pool.ntp.org	123	UDP	NTP
time1.google.com	123	UDP	NTP
time2.google.com	123	UDP	NTP
time3.google.com	123	UDP	NTP
time4.google.com	123	UDP	NTP
worldtimeapi.org	443	TCP	HTTPS
api.eu.vef.retail.interact-lighting.com	443	TCP	HTTPS
global.azure-devices-provisioning.net	443	TCP	HTTPS
irheuprd.azure-devices-provisioning.net	443	TCP	HTTPS
global.azure-devices-provisioning.net	5671	TCP	AMQP
irheuprd.azure-devices-provisioning.net	5671	TCP	AMQP
global.azure-devices-provisioning.net	8883	TCP	MQTT
irheuprd.azure-devices-provisioning.net	8883	TCP	MQTT
irheuprd0.azure-devices.net	443	TCP	HTTPS
irheuprd0.azure-devices.net	5671	TCP	AMQP
irheuprd0.azure-devices.net	8883	TCP	MQTT
mcr.microsoft.com	443	TCP	HTTPS
irheuprd.azurecr.io	443	TCP	HTTPS
yellowdoteuprd.blob.core.windows.net	443	TCP	HTTPS
irhdeviceseuprd.blob.core.windows.net	443	TCP	HTTPS
device-registration.dynalite.interact-lighting.com	443	TCP	HTTPS

Note

It's recommended to configure the public Google DNS server IP address (8.8.8.8) either as the primary or alternative DNS server on the PDDEG-S, and allow it on the firewall of the network. In case it's preferred to use any other public DNS server, make sure to add this IP address to the list of endpoints.

Endpoint	Port	Transport	Application
mqtt.dynalite.interact-lighting.com	443	TCP	HTTPS
mqtt.dynalite.interact-lighting.com	8883	TCP	MQTT
sqs.eu-central-1.amazonaws.com	443	TCP	HTTPS
sqs.ap-south-1.amazonaws.com	443	TCP	HTTPS
sqs.ap-southeast-1.amazonaws.com	443	TCP	HTTPS
sqs.ap-southeast-2.amazonaws.com	443	TCP	HTTPS
sqs.us-east-1.amazonaws.com	443	TCP	HTTPS
siteservicejobfiles.s3.eu-central-1.amazonaws.com	443	TCP	HTTPS
dynaliteprodjobfilerepo.s3.eu-central-1.amazonaws.com	443	TCP	HTTPS
dynalite.interact-lighting.com	443	TCP	HTTPS
irhveeuprd.servicebus.windows.net	5671	TCP	AMQP
eu.mqtt.iotplatform.signify.com	443	TCP	HTTPS
eu.api.iotplatform.signify.com	443	TCP	HTTPS
data-acq-macrobatch.dna.iotplatform.signify.com	443	TCP	HTTPS
data-acq-config.dna.iotplatform.signify.com	443	TCP	HTTPS
*.data.mcr.microsoft.com (see note)	443	TCP	HTTPS
*.iotplatform.signify.com (see note)	443	TCP	HTTPS
*.blob.core.windows.net (see note)	443	TCP	HTTPS

Note
The wildcard (*) indicates that the system uses multiple endpoints of this domain.

Find out more about Interact
www.interact-lighting.com

interact

R04, 14 October 2024