interact

IT configuration

Architecture PRF/PRA

Version v2.5

13 February 2024

Contents

1. Introduction

This section details the target audience and abbreviations used.

1.1. Target audience

PRF/PRA is aimed at small and medium enterprises (SME), often privately held.

The target audiences for this document are:

- Service provider/Installer
- Business owner/User

This section describes the IT design of the system and the prerequisites for the IT network of the customer.

It includes more detailed information about requirements of the IT network, wireless networking, user management and data collection.

1.2. Abbreviations

Abbreviation	Explanation
IoT	Internet of Things
IPv4	Internet Protocol version 4
SME	Small and Medium Enterprises
WG	Wireless Gateway, also called gateway

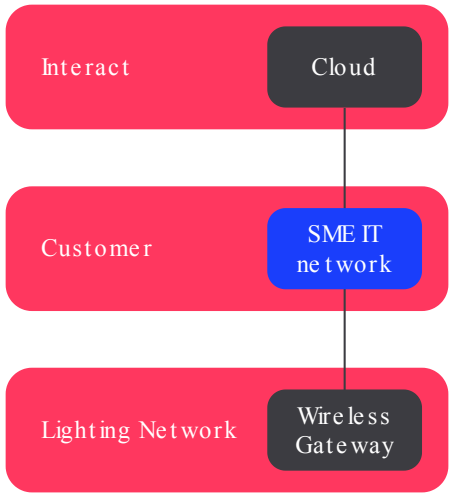
2. IT network requirements

In a wireless connected lighting system, much of the lighting control behavior is distributed over the devices (luminaire controller, Wireless Gateway) that compose the system.

The communication between the Wireless Gateway, that is connected to the IT network of the customer using an Ethernet connection, is done via secure protocols, where Zigbee is a wireless protocol enabling communication between the gateway and Zigbee devices (lights, ZGP sensors and switches).

2.1. IT integration

The currently tested deployment of the lighting network with the IT infrastructure of the customer and the Interact cloud is depicted in the following diagram:



The diagram details an IT integration connecting the lighting system with the gateway connected via the IT network of the customer to the cloud

2.2. Network connections

The Wireless Gateway must be connected to the IT infrastructure of the customer.

For this purpose, an ethernet port with live LAN, that ultimately enables a route via the network of the customer to the cloud, is required.

2.3. Network requirements

2.3.1. Network requirements

The Wireless Gateway communicates towards the cloud via the IT network of the customer using IPv4.

The gateway must receive an IP address from a DHCP server; configuration of the gateway in combination with a static IP address (which is less commonly used) is not possible.

The communication between the Wireless Gateway and the cloud requires HTTPS, which uses the standard TCP-port 443.

This port is commonly used for access to the internet via a web browser. However, it needs to be validated with an IT representative of the end-customer whether their network has standard measures in place to block access to wired LAN connections.

In that case, the block needs to be cancelled, preferably with unrestricted access to IP addresses on the internet.

As the gateway always sets up connections from the gateway to the cloud, this is secure and avoids problems with load balancers that are typically used by cloud providers.

The system also needs the UDP port **123** to be open. This port is used for time synchronizing using the Network Time Protocol (NTP).

If firewalls are used to protect the network of the endcustomer, it is necessary to make sure that the following hosts can be connected to:

- sme.interact-lighting.com for port 80 and 443
- mq.sme.interact-lighting.com for port 443
- web.mqtt.pro.interact-lighting.com for port 443

Note

Classical firewalls typical provide protection at address level rather than host name level. For that it is recommended to remove the restriction for the specific LAN port that is used to connect the gateway, or free up and address range used to map these host names.

Summary of requirements to connect the system:

- Ethernet port with live LAN, connected with the IT network of the customer
- IPv4 via DHCP server available
- Port TCP 80 and 443 opened on the router
- Port UDP 123 opened on the router

3. Network security

3.1. Wireless network

The wireless Zigbee network operates on the 2.4 GHz band, also used by for example Wi-Fi and Bluetooth.

Although Wi-Fi and Zigbee can coexist, it is best to separate the two to avoid interference that occurs at high traffic load.

3.1.1. Packages

Both systems do not transmit continuously, but in small packages, leaving room for others to transmit.

A Wi-Fi channel can be used by several computers at (virtually) the same time.

Packages sent over the wireless Zigbee network are very small and will never compromise the throughput of a Wi-Fi system.

The wireless Zigbee network can only be compromised by the Wi-Fi system if this system is used to the absolute maximum (on all channels), leaving only little room to transmit.

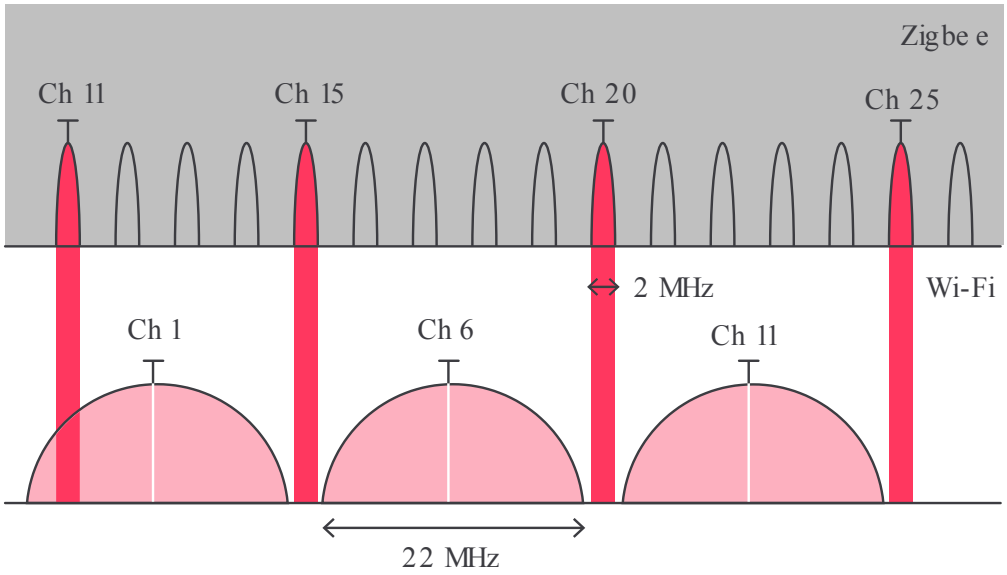
3.1.2. Channel selection

As Wi-Fi channels overlap each other, it is required to select non-overlapping channels to ensure best possible communication.

Interference between overlapping channels results in lower transmission speeds or at worst no communication at all.

In a well-managed Wi-Fi system, channels 1, 6 and 11 are used to create a network with full coverage without access points interfering with each other. Using these channels also leaves gaps in the frequency band.

The wireless Zigbee network uses channels 11, 15, 20 and 25 that are positioned in the gaps of the Wi-Fi band, as shown below:



3.1.3. Interference

Devices using Ultra High Frequency (UHF) radio signals are sensitive to interference. However, systems using frequencies in the 2.4 GHz band are designed to coexist.

Also, for the wireless Zigbee network, the transmitting powers are significantly lower when compared to Wi-Fi, mobile telephony etc. The table shows the relation between the maximum permitted powers for several types of radio signals.

Overview of maximum permitted powers for several appliances operating in UHF frequency bands

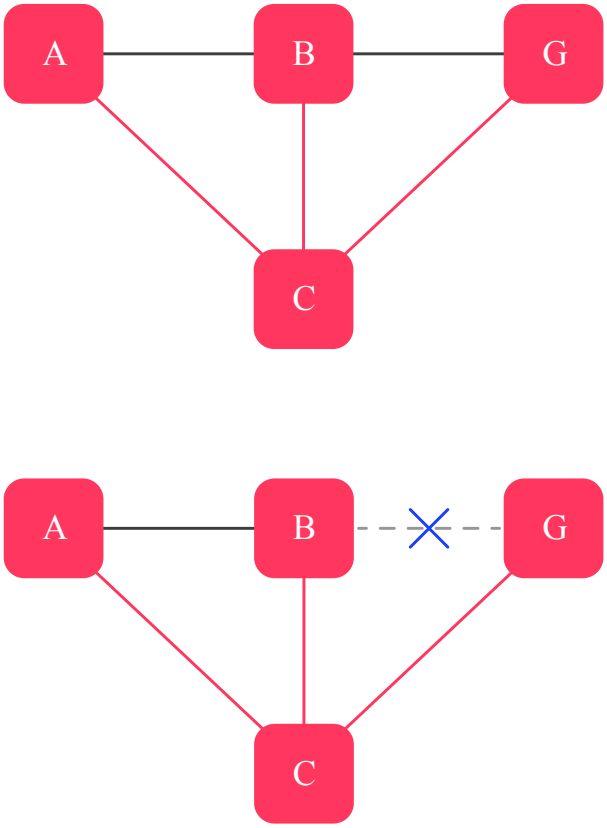
Device / Type	Max. permitted power	
	Transmitting power	Power ratio
Microwave	1000 W	60 dBm
Mobile telephone (GSM)	2 W	33 dBm
Wi-Fi (at 2.4 GHz)	100 mW	20 dBm
Bluetooth	100 mW	20 dBm
Zigbee	2.5 mW	4 dBm

3.1.4. Operational distances of Zigbee devices

Wireless Zigbee devices (gateway, sensors and ZGPs) are guaranteed to work up to a distance of 10 m (33 ft) between the devices.
Larger distances often work depending on the environment, but are not guaranteed.

3.1.5. Routing between wireless devices

The lights of a wireless system are guaranteed to work if the distance between the light and at least one of the other lights in the network is less than or equal to 10 m. It is preferred to have at least two lights within the range of each light, as the wireless Zigbee network uses mesh routing, as shown below:



Zigbee routing between wireless devices

This makes the network much more robust as multiple routing paths can be used for communication.

The connection from light A to the gateway G can go via light B. If for some reason the connection between A and B is blocked, the network will automatically route the traffic through light point C.

These require the light to be installed within the reach of at least two other lights within 10 m (33 ft).

As the Zigbee Green Power devices (sensors and switches) only send messages in the Zigbee network, they exist in the network, but play no role in the routing between the wireless devices.

3.2. Security considerations

The design of a (wireless) connected lighting system takes the following main threats and mitigations into consideration:

Overview of vulnerabilities and mitigations

Vulnerability	Mitigation
Changing configuration of the lights	Limited (physical) access to the lights and gateway
Interfering with the lighting control protocol	Limited (physical) access to the lights and gateway
Changing the network configuration of the lighting system	Secure communications of the lighting devices
Unauthorized data retrieval from the lighting system	User management on tools using Role Based Access Control
	Secure communications to the Portal
Unauthorized access to the Portal and App	User management on tools using Role Based Access Control
	Secure communications to the Portal

3.2.1. Description of vulnerabilities

Detailed description of the main threats identified in the design of the system.

Changing configuration of the lights

The lights need a specific set of configuration parameters. For the correct functioning of the lighting system this may not be interfered with.

Interfering with the lighting control protocol

The components in the lighting system exchange control messages to change the status of the lighting system. For the correct functioning of the system this may not be interfered with.

Changing the network configuration of the lighting system

The lighting system is configured in such a way that the components can find each other and communicate. For the reliable operation of the lighting system, this should not be interfered with.

Unauthorized data retrieval from the lighting system

The lighting system gathers information from sensors and status from its components. This information may be valuable and shall therefore be accessed only by authorized persons or entities.

Unauthorized access to the Portal and App

Via their interfaces, the Portal and App provides full control and management of the lighting system as well as the lighting and system data. For secure and reliable operation of the system, access to these interfaces shall only be allowed to authorized persons or entities

3.2.2. Description of mitigations

Detailed description of the mitigations and secure configuration options of the system.

Limited (physical) access to the lights and gateway

Lights and sensors will in general be located in the ceiling of the rooms, open areas and other indoor locations.
Furthermore, the maintenance access to the controllers in the lights is limited. The gateway must be positioned at visible locations at high altitude against a wall or ceiling.

User management on tools using Role Based Access Control

Access to the Portal and App is controlled via user accounts. These user accounts are created and managed in the portal. The following roles are being used:

- The service provider serves as an administrator of all projects in his portfolio, including user management of all types of users:
  - Administrator (identical to service provider)
  - Installer
  - Owner
  - User
- The installer installs and commissions the lighting system and can setup the following types of users of projects he is assigned to:
  - Owner
  - User
- The owner uses, serves as an administrator to the system he owns, controls and monitors the lighting system, and manages the users:
  - Administrator (identical to owner)
  - Installer (owner can revoke access to an installer)
  - User
- The user can only control (a limited number of areas of) the lighting system.

Secure communications to the Portal

Access to the Portal secured via HTTPS (TLS 1.2). The security of HTTPS provides authentication of the server towards the clients as well as protection for all information that is transferred.

Secure communications of the lighting devices

The gateway has a product key programmed in the device. The product keys are registered in the production cloud of the connected lighting system.

During the localization process, the product key is authenticated by means of a QR code. Only the installer that is authorized and logged in with the correct user credentials can authenticate the gateway during commissioning.

During network creation, the Zigbee devices use a TrustCenter (gateway) and can only be added when discovered in the lighting network. The installer however must be logged in with an account for the appropriate project to be able to select the fixtures in the tool. Adding devices to the system without the correct authorizations is not possible.

The Zigbee communication is secured by encrypting all messages that are exchanged using AES with a local secret key.

4. Data collection

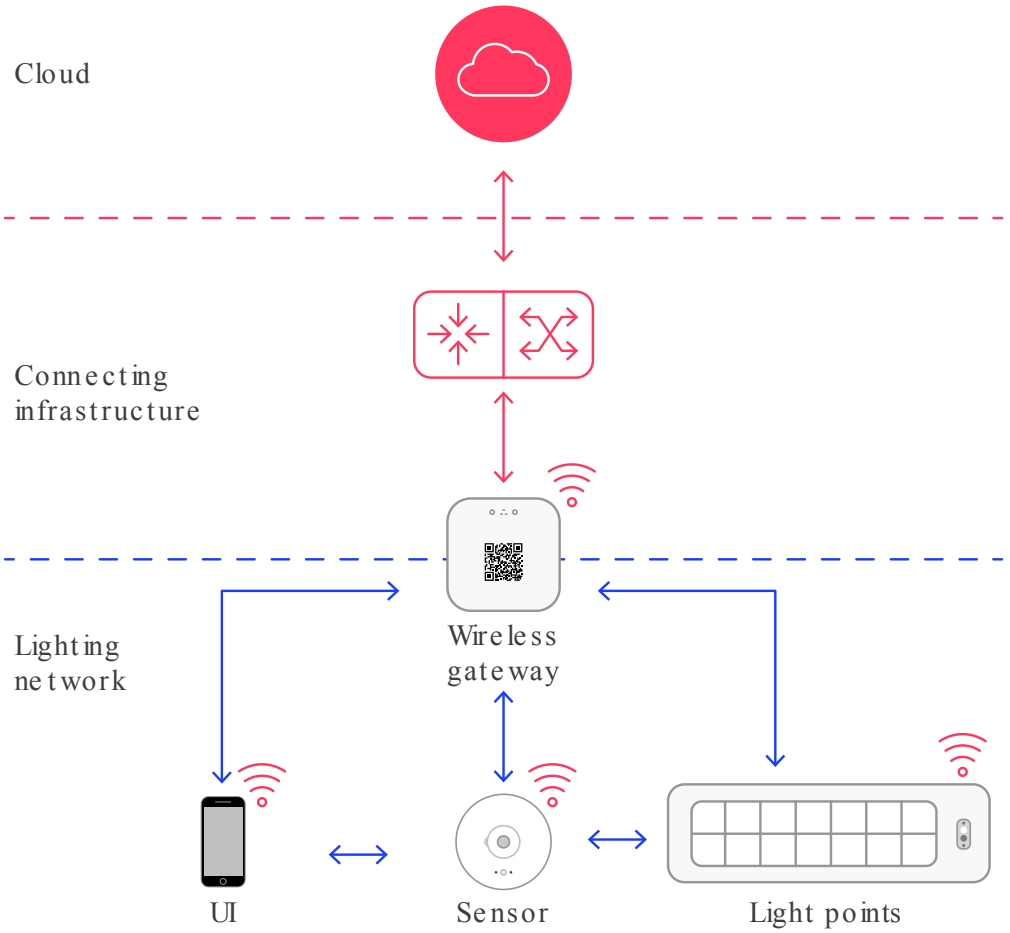
4.1. Data collection

A connected lighting system collects various types of data. The gateway collects all the data from the devices that correspond with it. This data is stored internally and forwarded to the cloud, to be used to create graphical representations in the Installer and Customer dashboard.

The gateway collects data measured in some way in the end devices. There are two types of data communication:

- Data that is polled by the gateway. Actively retrieve relevant data from the associated lights, including the polling frequency.
- Data that is evented from the lights to the gateway.

Devices send relevant data as an event to the gateway. Data collected this way is for example the energy consumption and status information.



Both polling and event data are communication setup between the gateway and field devices.

The gateway also checks regularly if its associated devices are still present. If not, it tries to reconnect several times and if these all fail, it will send an alarm, which will be shown on the dashboard. The gateway keeps track of the connection status of the lights and reports it to the Portal.

The *sensing* capabilities supported by the system are:

- Light level (for daylight regulation), motion and infrared for light control
- Power and energy measurement in the light
- Operating hours of the light
- Device on-line/off-line for all field devices (lights)
- Device alarms

Learn more about Interact
www.interact-lighting.com