Installation manual Eaton Wireless SC Edge Controller – Cellular

Target Audience Part 1: Qualified electricians in accordance with EN 50110-1



Powering Business Worldwide

Table of Contents

1.General information 3

2.Cybersecurity notes.....3

3.Introduction / Foreword.....4

3.1. Technical data: 5

4.Installation step by step 5

4.1.Mounting on a wall : 5

4.2. Wire the Wireless SC edge controller..... 6

4.2.1. Power Wiring..... 6

4.2.2. Direct connection 6

4.2.3. With VisionGuard..... 7

4.2.4. Hybrid..... 7

4.2.5. Mains card 7

4.2.6. I/O Card 8

4.3. LED status 9

4.4. Install the Building Safety Manager – Mobile APP 9

1. General information

Please read the Safety Instruction sheet for information on:

- Safety instructions
- Conformity to standards
- Content of assembly and installation instructions
- Modifications and conversions
- Work safety

You can find this documentation under the Resources tab of the Wireless SC monitoring system Website:

https://www.eaton.com/de/en-gb/catalog/emergency-lighting/wireless-monitoring-system.html

2. Cybersecurity notes

This chapter provides guidelines to securely deploy the Wireless SC edge controller and minimize the cybersecurity risk to the installer system.

- **Asset identification and inventory:** Ensure that the Wireless SC edge controller is labelled and inventoried using the Part number, EPAS number and MAC address printed on the product label.
- **Restrict Physical access:** Ensure that physical access to the Wireless SC edge controller is restricted only to authorized user(s). Wireless SC edge controller supports the physical access ports RJ-45 and USB that can be used to tamper the device. Access to these ports should be restricted to authorized personnel only. Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate. Monitor and log the access at all times. Before connecting any portable device through a USB port or SD card slot, scan the device to prevent unauthorized access/malware.
- **Restrict Logical access:** Access to 'Admin' & 'Service' user accounts should be restricted to authorized personnel only as system configuration can be tampered by abusing these accounts. Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 8 characters, mix of upper- and lower-case and special characters, or otherwise in accordance with your organization's policies).

  As password protection is very important for protection against unauthorized or unwanted access by third parties, additional rules should be observed when assigning a password:

  - Change the default password of all devices.
  - Avoid names of family members, pets, best friends, favorite stars, or their birth dates or similar arrangements.
  - If possible, passwords should not appear in dictionaries.
  - It should not consist of common variants and repeat or keyboard patterns, i.e. not qwerty or abcd1234 and so on.
  - Appending simple numbers to the end of the password or placing one of the usual special characters (for example $! ? #) at the beginning or end of an otherwise simple password is likewise inadvisable
- **No account sharing:** Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security.
- **Leverage the roles / access privileges / Organization:** to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role).
- **Restrict Network Access:** Ideally the Wireless SC edge controller should be installed on a segregated network. However, when the Wireless SC edge controller is connected to a wider network, make sure that the IP address and MAC address are filtered at the router side, or using a firewall.
- **Logging and event management:** Log all relevant system and application events, including all administrative and maintenance activities. Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). Ensure that logs are retained for a reasonable and appropriate length of time. Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the Wireless SC edge controller and any data it processes. Logs are saved locally in EL system and on the cloud, and may be accessed via the Building Safety Manager web and mobile applications.
- **Secure maintenance:** In case the firmware of the device needs to be updated, an email and/or notification will be received, providing details are up to date and the system is covered by a Service plan.
- **Malware Defenses:** Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

- **Business continuity / cybersecurity disaster recovery:** Eaton recommends incorporating Wireless SC edge controller into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important device data should be backed up and securely stored, including the current configuration and documentation of the current permissions / access controls, if not backed up as part of the configuration. The Building Safety Management System can be used to save the configuration using the Building Safety Manager web and mobile applications.
- **Sensitive Information Disclosure:** Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by Building Safety Management System be adequately protected through the deployment of organizational security practices

The Wireless Emergency Lighting monitoring system has been designed with cybersecurity as an important consideration. A number of features are offered in this digital ecosystem to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.

The following whitepapers are available for more information on general cybersecurity best practices and guidelines:

[R1] Cybersecurity considerations for information and communication technology (WP152002EN):

https://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity best practices checklist reminder (WP910003EN):

https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

https://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R4] Cybersecurity Best Practices Checklist Reminder (WP910003EN):

https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

More information related to cybersecurity best practices is available on Eaton.com.

A copy of the End user license agreement (EULA) is available and accessible from the Building Safety Manager Web and Mobile Applications. The EULA may be viewed on creation of an account, and continued use of the account implies acceptance of the terms and conditions.

3. Introduction / Foreword

Eaton's Wireless Emergency Lighting monitoring system is a new Self-Contained monitored system based on the massive dynamic radio mesh network technology. Eaton's new, mobile app-controlled wireless emergency lighting monitoring system shortens installation times, as well as eliminating costly data cable fault-finding.

The system's single, high-capacity, cloud-connected mesh network is secured by a unique key and Eaton cybersecurity approved technology. It can run up to 1024 units in 16 digital zones over multiple floors. Luminaires are either digital native wireless with embedded radio or selected from the proven, wide CGLine+ range and fitted with a wireless emulator module.

Easy commissioning and maintenance are via Building Safety Manager, Eaton's intuitive mobile app available in Android and iOS. Fully integrated into Eaton's building safety management system (BSMS), this complements a similarly user-friendly web app for remote monitoring, email notifications and logbook access.

Eaton's high-capacity wireless emergency lighting system delivers cable-free convenience, fingertip remote control and best-in-class security.

Based on Building Safety Management System (BSMS), Eaton's Wireless Emergency Lighting monitoring system is a new, full lifecycle digital experience for Monitored Self-contained emergency lighting.

Eaton's Wireless Emergency Lighting monitoring system is part of the Brightlayer suite and consist consists in:

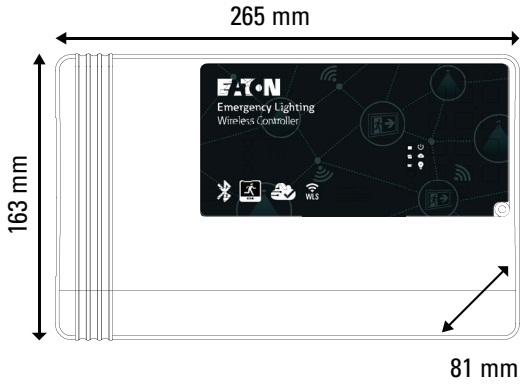
- Building Safety Manager - Mobile App
- Building Safety Manager - Web App
- Building Safety Manager - Cloud
- Building Safety Manager – Analytics
- Wireless SC edge controller

3.1. Technical data:

CTR1024WLSCS =

Wireless SC edge controller SIM IP - Cellular

Power supply (typ.)	220-240V, 50/60Hz
Power Consumption	<18W full load (RMS)
Connection terminals	max. 1.5mm² flexible
Permissible ambient temperature	0°C ... +35°C
Storage temperature	0°C ... +35°C
Protection rating	IP20



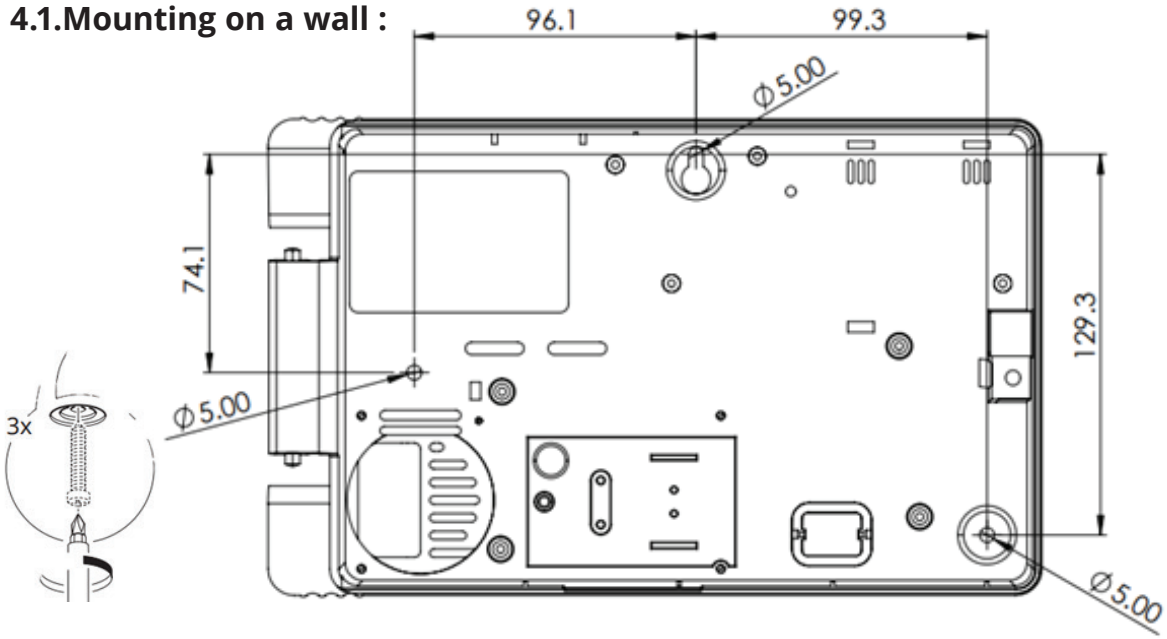
4. Installation step by step

Building Safety Manager - Mobile APP is mandatory to connect to the Wireless SC edge controller and to perform commissioning and setting.

The user interface (UI) is very simple to use and partially automated, requiring minimal effort from the Technician to configure the Wireless SC edge controller.



4.1.Mounting on a wall :

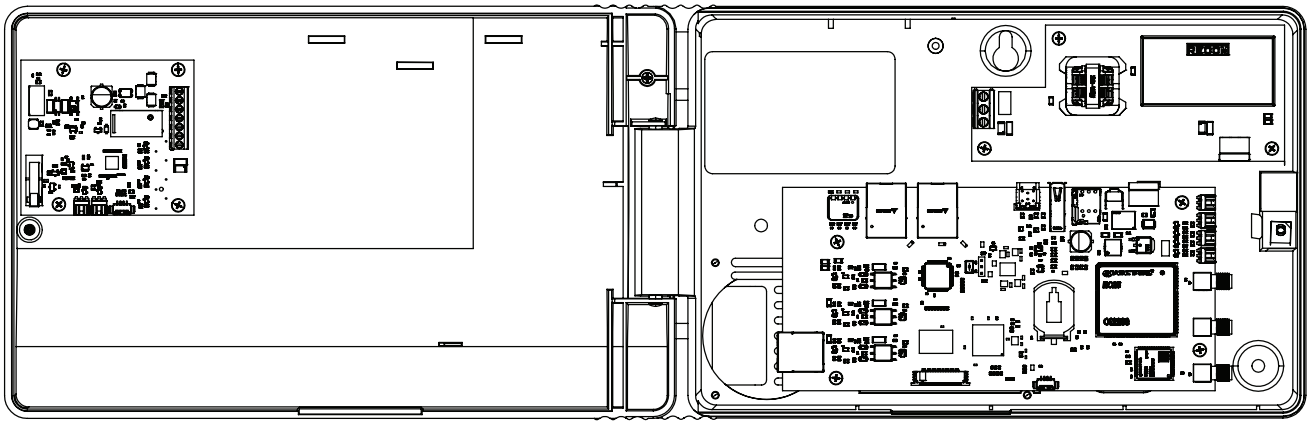


4.2. Wire the Wireless SC edge controller

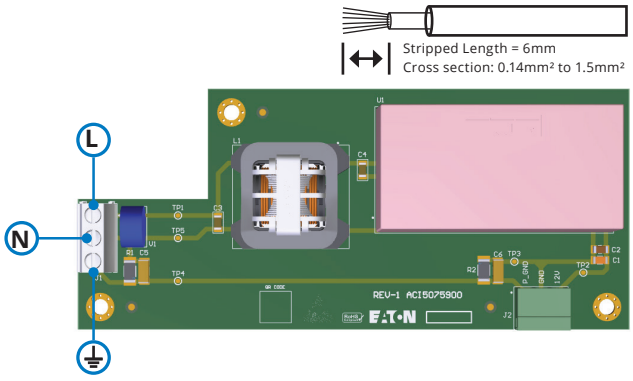
DANGER!

Only skilled or instructed persons may carry out the following operations.

There are 3 options for connecting emergency lighting systems to the Wireless SC edge controller and completing the commissioning. Choose the appropriate commissioning process based upon your intended setup.

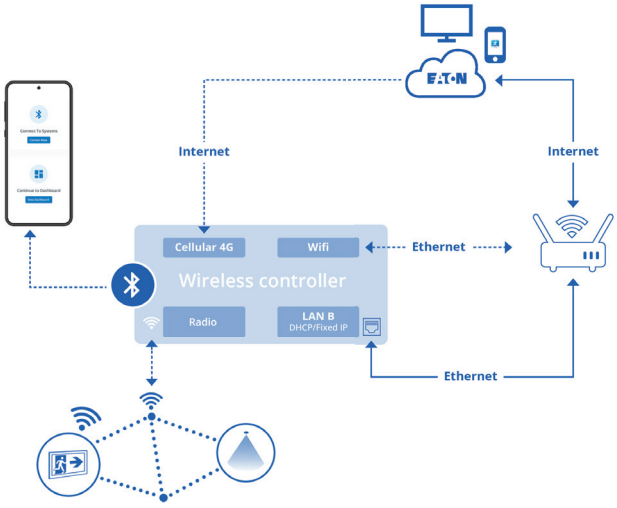


4.2.1. Power Wiring



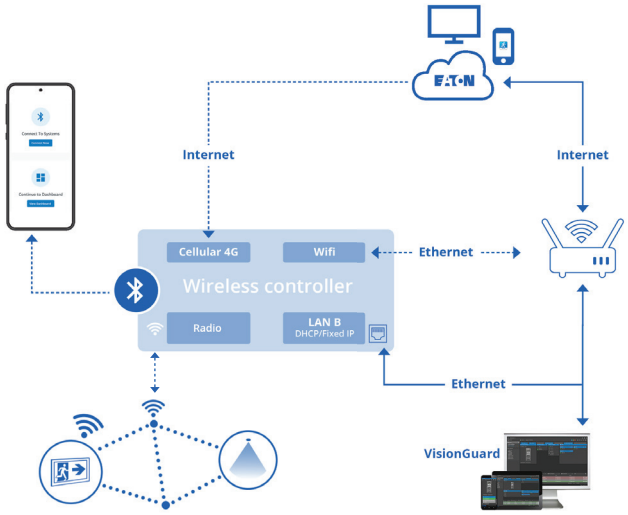
4.2.2. Direct connection

(only BSMS)



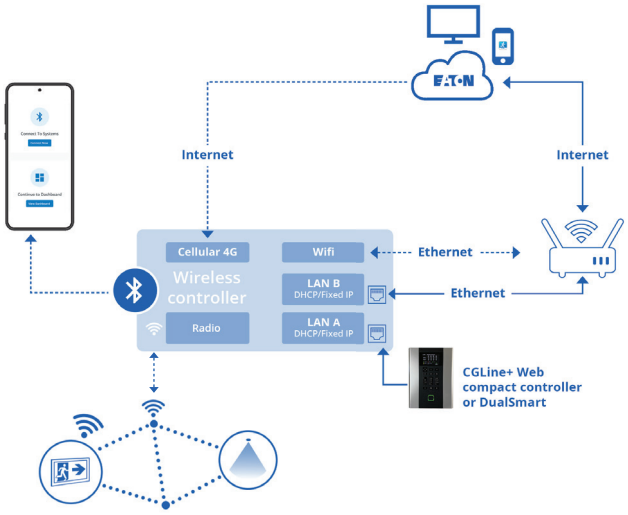
4.2.3. With VisionGuard

(Need to be connected to the same IP network)



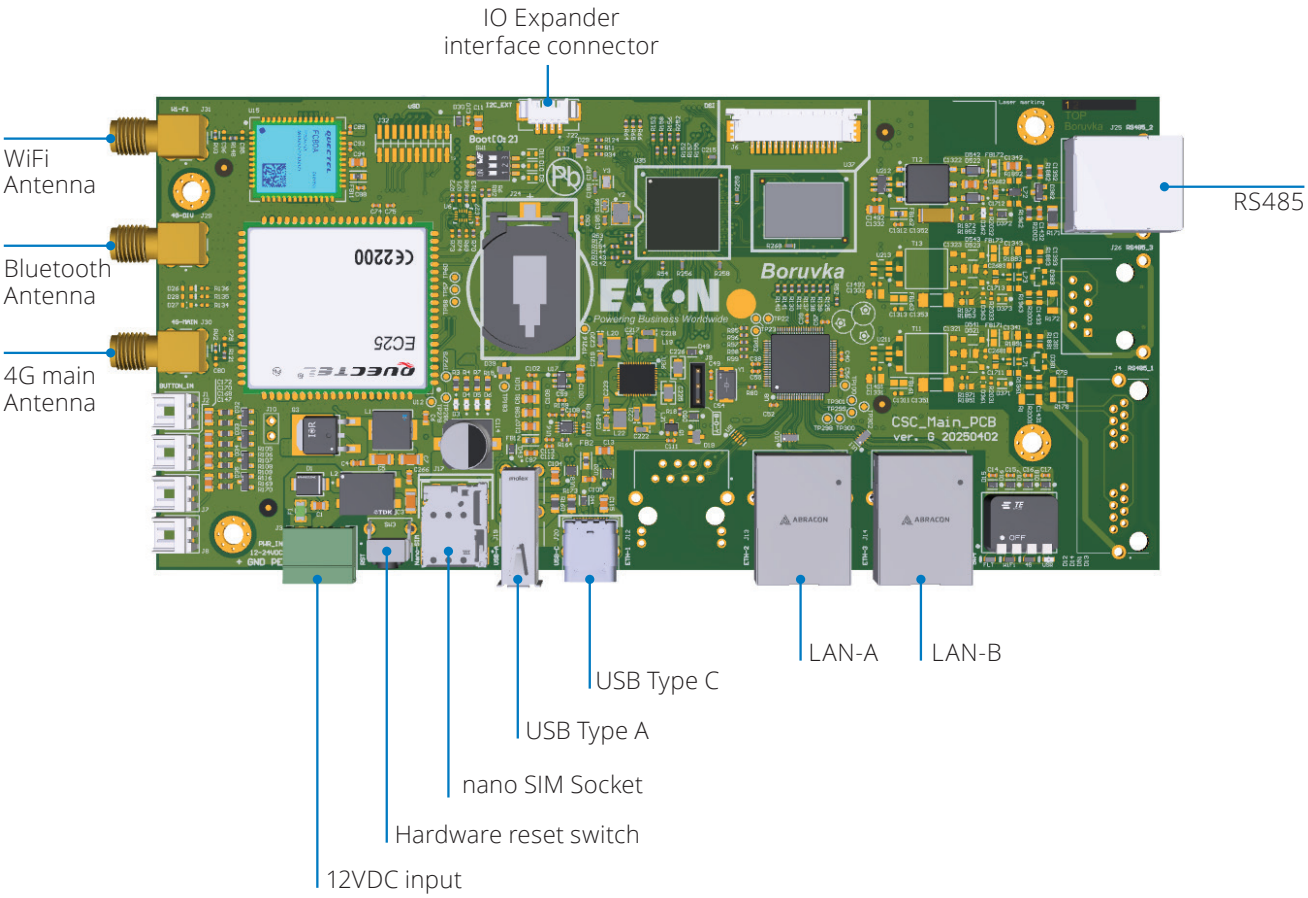
4.2.4. Hybrid

(Dual EL systems)

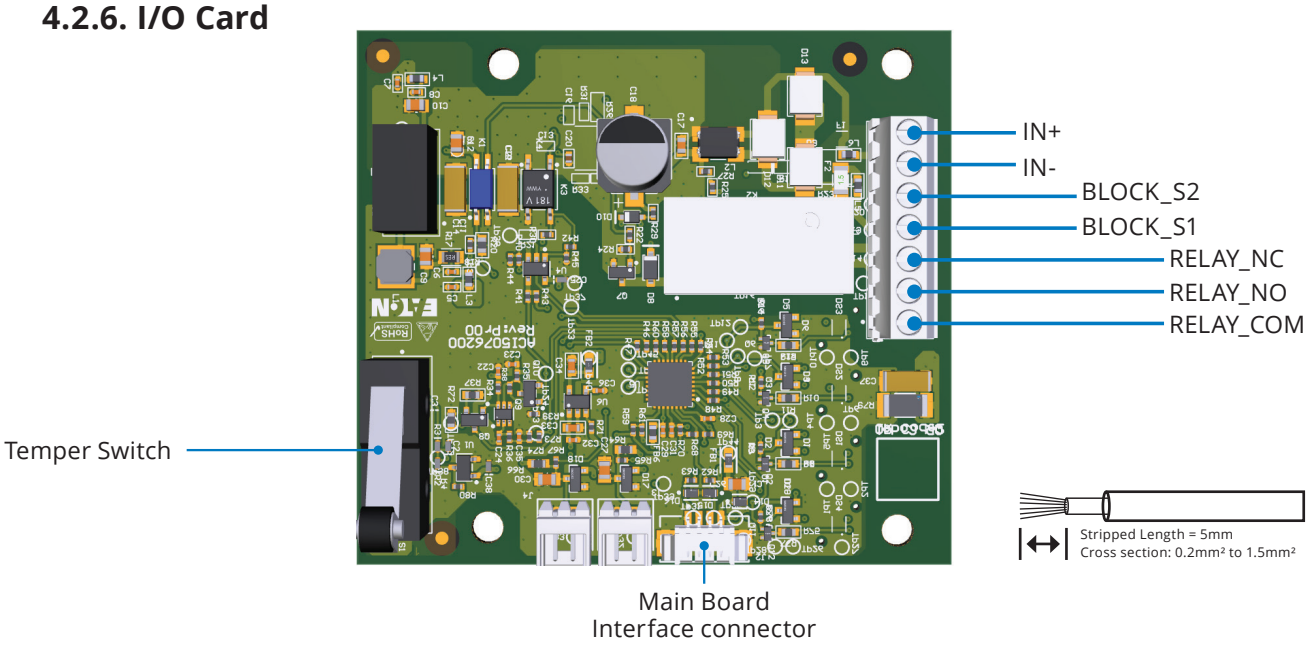


LAN B default parameters
DHCP Automatic
IP address: 192.xxx.xxx.xxx ?
Subnet mask 255.255.xxx.xxx ?

4.2.5. Mains card



4.2.6. I/O Card



Programmable digital inputs

The inputs are activated by bridging of both contacts of In1 or In2. The following functions can be freely assigned to the digital input:

- Activate IA mode (System or Zones)
- Maintained mode OFF (System or Zones)
- Start function test (System or Zones)
- Stop test
- External failure

Relay outputs:

The Wireless edge controller also has a freely programmable relay output each with a change-over contact. Programmable functions:

- At least one luminaire failure
- Several consecutive luminaire failures
- Communication failure
- Battery operation
- Function test active
- Duration test active
- Charging failure
- Test failure

The contacts of the Relay must be used within the voltage limit of ES1 (Udc<15V).

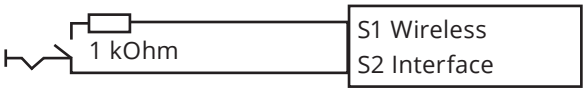
Blocking input (S1/S2)

All connected luminaires can be blocked via the blocking input, meaning the luminaires are switched off and the emergency light function deactivated, for example for idle operating times.

Connection is via a key switch or relay (e.g. alarm system). To guarantee reliable operation from short-circuit or interruption of the blocking line, this input is equipped with differential loop monitoring (static current), meaning a 1kOhm resistance must be integrated for blocking that defines the static current.

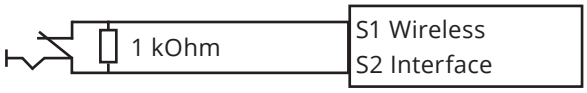
Connection example:

With closer contact



Resistor must be connected next to the switch.

With opener contact



Resistor must be connected next to the switch.

4.3. LED status



	Status / Statut		LED
Power ⏻	Power	●	lights up green
	Connected with Building Safety Manager - mobile App (Priority 1)	✸	blinks orange
	Firmware update requested (Priority 2)	●	lights up orange
	Product is off	❍	LED is off
System	Ready	●	lights up green
	Not commissioned / no luminaire associated (Priority 1)	✸	blinks orange
	Offline / not connected to Internet (Priority 2)	●	lights up orange
Luminaires	Ready	●	lights up green
	Test in progress (Priority 1)	✸	blinks green
	Identification in progress (Priority 2)	✸/✸	blinks green / orange
	Blocked (Priority 3)	●	lights up orange
	Failures / warning (battery failure, lamp failure, com failure) (Priority 4)	✸	blinks orange

4.4.Install the Building Safety Manager – Mobile APP

Requested to perform the commissioning

For further information on the installation process please read the **Wireless Quick Start Guide** or watch our **"How to" videos** on commissioning steps.

Notes

Eaton is an intelligent power management company dedicated to protecting the environment and improving the quality of life for people everywhere. We make products for the data center, utility, industrial, commercial, machine building, residential, aerospace and mobility markets. We are guided by our commitment to do business right, to operate sustainably and to help our customers manage power – today and well into the future. By capitalizing on the global growth trends of electrification and digitalization, we're accelerating the planet's transition to renewable energy sources, helping to solve the world's most urgent power management challenges, and building a more sustainable society for people today and generations to come.

Eaton was founded in 1911 and has been listed on the New York Stock Exchange for more than a century. We reported revenues of $23.2 billion in 2023 and serve customers in more than 160 countries. For more information, visit www.eaton.com. Follow us on LinkedIn.

Eaton
EMEA Headquarters
Route de la Longeraie 7
1110 Morges, Switzerland
Eaton.eu

CEAG Notlichtsysteme GmbH
Senator-Schwartz-Ring 26
59494 Soest, Germany
Tel.: +49 (0) 2921 69-870
Fax: +49 (0) 2921 69-617
Email: info-n@ceag.de
Website: www.eaton.com

© 2025 Eaton
All rights reserved
Printed in Germany
Article no. 40071860667
Publication number IL454002ML
September 2025

Eaton is a registered trademark.

All other trademarks are the property of their respective owners.

www.eaton.com/recycling

Powering Business Worldwide