Edge Gateway 800 Series

Version:
v1.1.0

Date:
17.11.2025

Contents

1 Copyright

2 Regulatory Compliances

2.1 CE and UKCA Notice

This device complies with the requirements of the CE directive and UKCA regulations.

Low Voltage Directive 2014/35/EU + Electrical Equipment Safety Regulations 2016 (SI 2016 No 1101)

- EN IEC 62368-1:2020+A11:2020
- BS EN IEC 62368-1:2020+A11:2020

EMC Directive 2014/30/EU + Electromagnetic Compatibility Regulations 2016

- EN 55032:2015+A11:2020
- BS EN 55032:2015+A11:2020
- EN 55032:2015+A11:2020
- BS EN 55032:2015+A11:2020
- EN IEC 61000-3-2:2019
- BS EN IEC 61000-3-2:2019+A1:2021
- EN 61000-3-3:2013+A1:2019
- BS EN 61000-3-3:2013+A1:2019+A2:2021
- EN 55035:2017+A11:2020
- BS EN 55035:2017+A11:2020
- EN 61000-4-2:2009
- BS EN 61000-4-2:2009
- EN 55035:2017+A11:2020
- BS EN 55035:2017+A11:2020
- EN 61000-4-3:2009
- BS EN 61000-4-3:2009
- EN 61000-4-3:2006+A1:2008+A2:2010
- BS EN IEC 61000-4-3:2020
- EN 61000-4-4:2012
- BS EN 61000-4-4:2012
- EN 61000-4-5:2014+A1:2017
- BS EN 61000-4-5:2014+A1:2017
- EN 61000-4-6:2014
- BS EN 61000-4-6:2014
- EN 61000-4-8:2010
- BS EN 61000-4-8:2010
- EN 61000-4-11:2004

- BS EN 61000-4-11:2004

RoHS 2 Directive 2011/65/EU & 2015/863/EU + RoHS 2 Directive 2020 No. 1647

- Exemption(s) used:
- 6c,7a,7c-I

2.2 FCC PART 15 VERIFICATION STATEMENT

WARNING

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

2.3 ICED-003 ISSUE 7 VERIFICATION STATEMENT

CAN ICES3(B)/NMB3(B)

This device complies with CAN ICES-003 Issue 7 Class B. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

3 Intended Use and IT Security Instructions

This section provides crucial safety and security information and recommendations to help you configure your Welotec IoT Edge Gateway (Edge Gateway) for optimal security in your deployment.

3.1 Intended Use

This section specifies the intended use and essential operating conditions for your Welotec IoT Edge Gateway (hereinafter referred to as “Edge Gateway”).

The Edge Gateway is consisting of a compute hardware and the Yocto-based Linux OS “egOS”. While the Edge Gateway itself has a limited and well documented feature set, applications can be deployed to the product exclusively as Docker Containers - these applications are not being delivered or maintained by Welotec, but by the customer himself or a third party chosen by the customer. In general the OS feature set is identical for all the models of the Edge Gateway Series, the scope of the features depends on model due to differences in interfaces.

The Edge Gateway is designed for use as a dedicated control, monitoring, and data acquisition unit within the enclosed control cabinet of a machine. Its primary function is to execute specific machine-control software, process operational data, provide human-machine interface (HMI) functionalities, and/or facilitate communication within the industrial automation environment. The Edge Gateway is exclusively intended for continuous operation within a controlled industrial setting.

The intended use of the Edge Gateway is strictly defined by the following conditions and requirements:

3.1.1 Physical Security and Installation Environment

- Enclosure: The Edge Gateway must be permanently installed within a secure, locked control cabinet (e.g., meeting IP54 or higher protection class) that provides adequate protection against dust, moisture, mechanical impact and unauthorized access.
- Controlled Access: Access to the control cabinet and its wiring must be restricted to authorized personnel only. Physical security measures (e.g., key locks, access control systems) are mandatory.
- Environmental Conditions:
  - Temperature: The Edge Gateway must operate within the specified ambient temperature and humidity range as outlined in the technical specifications. Adequate ventilation or active cooling within the cabinet must ensure these limits are not exceeded. This includes accounting for the unit’s own thermal dissipation and that of all other components in the cabinet.
  - Vibration and Shock: The Edge Gateway must be mounted securely within the cabinet to minimize exposure to excessive vibrations and mechanical shock, adhering to the manufacturer’s specifications.
  - Cleanliness: The inside of the cabinet must be kept free of dust, debris, and contaminants that could impair cooling or lead to electrical shorts.

3.1.2 EMC compliant electrical Installation and Power Supply

This product is designed to meet EMC standards when installed according to the following instructions. Failure to adhere to these instructions may result in the equipment failing to meet compliance standards and can cause interference with other devices. The installer is responsible for ensuring the EMC conformity of the final system.

- Power Supply: The Edge Gateway must be connected to a dedicated stable and filtered power supply within the specified voltage range. To ensure operational reliability and meet EMC requirements, the power source must provide adequate filtering against surges, transients, electrical fast transients (EFTs), and conducted RF noise common in industrial environments. An Uninterruptible Power Supply (UPS) is highly recommended to protect further against power fluctuations and outages.
- Wiring: All wiring connecting to the Edge Gateway must comply with applicable industrial wiring standards, be properly insulated, strain-relieved, and protected against mechanical damage.
- Grounding: The unit must be properly grounded according to the installation manual, typically via a low-impedance connection to the control cabinet's central grounding point.

3.1.3 Functional Safety

This unit is not certified as a standalone component for functional safety applications (e.g., SIL, PL).

Intended Use: The unit is intended for standard control and monitoring. It must not be used as the sole or primary controller for safety-critical functions (e.g., emergency stops, safety interlocks, light curtains, burner controls).

System Integration: Safety-related control logic must be executed by dedicated, certified safety controllers (e.g., Safety PLC, safety relays). This unit may be used to supervise or monitor a safety system (e.g., for HMI visualization or data logging) via a non-safety-rated communication channel, but it must not be part of the safety-critical control loop. The failure of this unit must not lead to a loss of the primary safety function.

3.1.4 Qualified and Trained Personnel

- Installation, Configuration, and Maintenance: All installation, configuration, maintenance and troubleshooting on the Edge Gateway and its connections within the control cabinet must be performed exclusively by qualified, trained, and authorized technical personnel. This personnel must possess proven expertise in electrical systems, IT hardware, and cybersecurity best practices.
- Security Awareness: All personnel interacting with the Edge Gateway or the network it is connected to must receive regular training on IT security awareness including password policies and reporting suspicious activities.

3.1.5 Secure Configuration

Secure Configuration: The Edge Gateway's operating system, firmware, and installed applications must be configured according to secure hardening guidelines, including disabling unused services, ports, and protocols, and enforcing strong password policies.

Please refer to the section "Cyber Security" for further details.

3.1.6 Network Segmentation and "Defense in Depth" IT Security Principles

- Network Segmentation: The unit and its control network must be isolated from all other networks (e.g., corporate, guest, public internet) using industrial firewalls and network segmentation. Direct connection to the internet is considered misuse unless done via a secure, managed gateway.
- Defense in Depth: A multi-layered security approach ("Defense in Depth") must be implemented for the entire system. This includes:

  - Network Security: Industrial Firewalls (e.g., Next-Generation Firewalls) at network boundaries, strict firewall rules (whitelist approach – only allow explicitly required traffic), VLANs for segmentation.
  - System Security: Configuration hardening (minimum services, disabled unnecessary ports), regular security updates and strong password policies.
  - Application Security: Secure configuration of all industrial applications, disabling default credentials, and ensuring application-level security features are enabled.
  - Data Integrity: Measures to ensure data integrity and availability (e.g., backups, redundant systems where appropriate).
  - Physical Security: see above
- Access Control: Remote access to the Edge Gateway (if required) must be strictly controlled, using secure connections, multi-factor authentication, and granular user permissions. Unnecessary remote access functionalities must be disabled.

3.2 Non-Intended Use

Any use of the Edge Gateway that deviates from the conditions described including but not limited to:

- Operation outside the specified environmental limits.
- Operation without a secure, enclosed control cabinet.
- Operation in hazardous locations (e.g., explosive atmospheres) for which the unit is not explicitly certified.
- Installation or maintenance by unqualified personnel.
- Connection to an unfiltered, unstable, or non-grounded power source.
- Direct connection to unsecured corporate networks or the internet without adequate protective measures.
- Installation of unauthorized software.
- Bypassing or disabling of security features (e.g., firewall).
- Failure to implement a cyber security management plan (patching, hardening, access control).

is considered non-intended use and may result in:

- Damage to the Edge Gateway or the machine.
- Compromised data security and integrity.
- Serious personal injury or death.
- Failure to comply with regulatory requirements.

3.3 Exposed Interfaces and Services

In factory default setting the following interfaces and services are exposed:

Interface	Service
LAN 1 … 4	SSH
COM 1 … 4	CLI
USB 1 … 6	n/a
HDMI 1 and 2	CLI
DP 1 and 2	CLI

In general available services highly depend on running applications and device configuration.

3.4 Cyber Security

Edge Gateways are being delivered with “egOS” - a Linux operating system designed specifically for edge applications with the highest security requirements. Its stability, reliability and security are achieved through regular updates and patches. The system is optimized for building a scalable IIoT infrastructure with integrated cloud connectivity and container runtime, and fully manageable via SMART EMS.

The following points have to be taken into consideration for secure installation and operation of the Edge Gateway:

3.4.1 Secure Boot

The Edge Gateway is equipped with Secure Boot mechanisms.

3.4.2 Storage Encryption

The Edge Gateway’s Storage is Encrypted.

3.4.3 Use Strong Passwords

Strong passwords are the first line of defense against unauthorized access. If you want to use password based access it is recommended to:

- Change the factory default password on first login
- Use passwords with a minimum length of 12 characters or more
- Use a combination of uppercase and lowercase letters, numbers, and special characters (e.g., !@#$%^&*)
- Do not use easily guessable patterns, such as sequences (e.g., “123456”, “abcdef”), repeated characters (e.g., “aaaaaa”), or dictionary words

3.4.4 System Hardening

The Edge Gateway’s configuration must be hardened by:

- Enforcing strong, unique passwords for all accounts.
- Implementing a least-privilege access model for users and applications.
- Configuring the OS-level firewall.

3.4.5 Patch Management

A robust process must be in place for testing and deploying security patches for the operating system and all deployed third-party applications. This process must be compatible with the operational constraints of the industrial environment. We recommend using SMART EMS for automated configuration and firmware updates as well as template-based management of devices.

3.4.6 Physical Security

Use of the locked control cabinet (see Section 3) to prevent unauthorized physical access and tampering (e.g., via USB ports) is a critical part of the security model.

3.5 Vulnerability Handling

Welotec has implemented a Coordinated Vulnerability Disclosure Policy - please visit the following site for further details: https://welotec.com/pages/coordinated-vulnerability-disclosure-policy

4 Safety Instructions

Please read these instructions carefully and retain them for future reference.

1. Disconnect this equipment from the power outlet before cleaning. Do not use liquid or sprayed detergent for cleaning. Use a moist cloth or sheet.
2. Keep this equipment away from humidity.
3. Ensure the power cord is positioned to prevent tripping hazards and do not place anything on top of it.
4. Pay attention to all cautions and warnings on the equipment.
5. If the equipment is not used for an extended period, disconnect it from the main power to avoid damage from transient over-voltage.
6. **Prolonged usage with less than 8V may damage the PSU or destroy the mainboard.**
7. Never pour any liquid into openings as this could cause fire or electrical shock.
8. Have the equipment checked by service personnel if:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture in a condensation environment.
    - The equipment does not function properly, or you cannot get it to work by following the user manual.
    - The equipment has been dropped and damaged.
9. Do not leave this equipment in an unconditioned environment, with storage temperatures below -20 degrees or above 60 degrees Celsius for extended periods, as this may damage the equipment.
10. Unplug the power cord when performing any service or adding optional kits.
11. Lithium Battery Caution:
    - Risk of explosion if the battery is replaced incorrectly. Replace only with the original or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
    - Do not remove the cover, and ensure no user-serviceable components are inside. Take the unit to a service center for service and repair.

⚠ Warning!
Always completely disconnect the power cord from your chassis whenever you work with the hardware. Do not make connections while the power is on. Sensitive electronic components can be damaged by sudden power surges. Only experienced electronics personnel should open the PC chassis.

⚠ Caution!
Always ground yourself to remove any static charge before touching the CPU card. Modern electronic devices are very sensitive to static electric charges. As a safety precaution, use a grounding wrist strap at all times. Place all electronic components in a static-dissipative surface or static-shielded bag when they are not in the chassis.

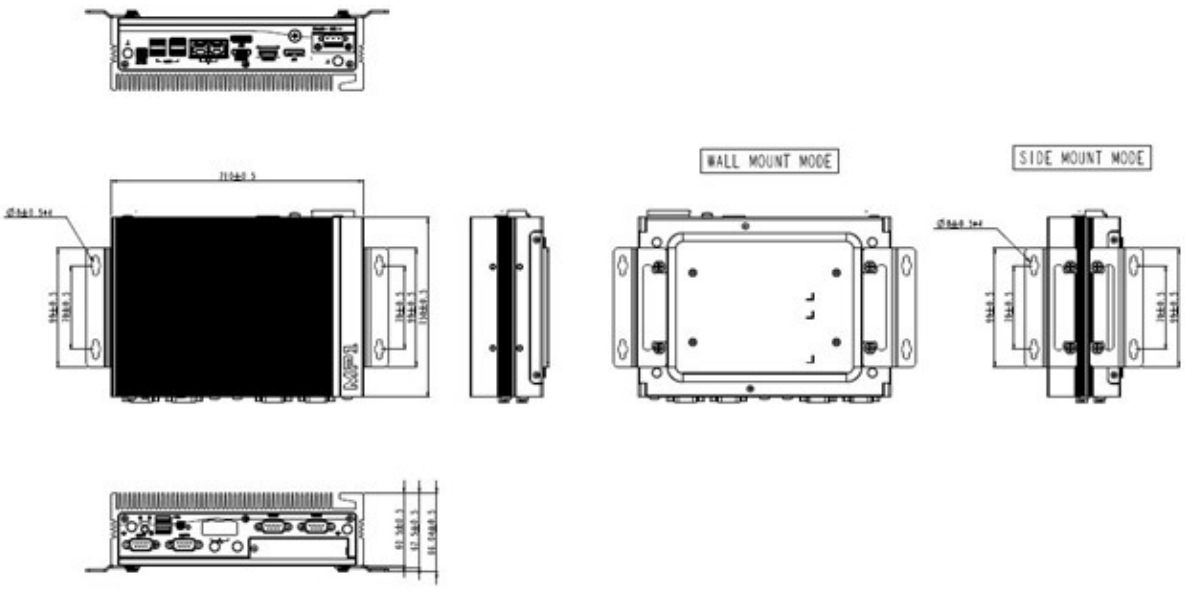
5 Product Specifications

5.1 Technical Details

Feature	Specification	Details
Processor	CPU	11th Gen Intel® Tiger Lake-UP3 Core™ i5-1145G7E – Quad Core, 8MB Cache, up to 4.10 GHz
Security	TPM	TPM 2.0 (Integrated Trusted Platform Module for secure device provisioning and authentication)
Memory	System Memory	16 GB RAM
Graphics	GPU	Intel® Iris Xe Graphics
Display	Display Interfaces	2 × HDMI, 2 × DisplayPort
Storage	Storage Capacity	240 GB free storage for container and data; optional: expandable up to 1 TB
Networking	Ethernet	2x (1x Gigabit LAN & 1x 2.5 Gigabit LAN) or 4x (3x Gigabit LAN & 1x 2.5 Gigabit LAN)
Expansion	USB Ports	4 × USB 3.1, 2 × USB 2.0
	Serial Ports	3 × RS-232, 1 × RS-485
Operating System	OS Support	Welotec egOS: hardened Linux operating system based on Yocto with no root access for users. Optional with HMI functionality
Software Features	Application Deployment	Docker CLI, Docker Compose, Moby Engine, Azure Edge Runtime
	Cloud Compatibility	Azure IoT Edge 1.4 and higher (native in OS), Azure IoT Hub, Azure DPS, AWS Greengrass 2.0 (via Container)
	Security Features	Integrated firewall, TPM 2.0, no root access for users, signed firmware images (with egOS 1.5 and higher)
	Network Features	Routing, NAT, 4G LTE Cellular Management, Wi-Fi Client support, Interface Management
Configuration	Remote Configuration	SMART EMS for configuration management, OTA firmware upgrade, certificate management
	Remote Access	VPN Security Suite for remote access and maintenance for the device and connected endpoint devices like PLC, HMI, IPC, and more
	Local Access	CLI via serial or SSH, local web interface for configuration (device onboarding in restricted company networks)
Power	Power Input	8–24V DC (+/- 10%) via 3-pin terminal block
	Power Supply (EU)	WIPC05000361
Mechanical	Mounting	Wall mount; DIN Rail mount (option WIPC09002890)
	Dimensions	210 mm (H) × 150 mm (D) × 63 mm (W); with DIN rail: 210 mm (H) × 150 mm (D) × 77 mm (W)
	Weight	2200 g
	Housing Material	Steel / Aluminum
	Ingress Protection	IP20
Environmental	Operating Temperature	-40°C to +60°C
	Storage Temperature	-40°C to +85°C

5.2 Dimensions

5.2.1 System Drawings



6 Power Supply

Use the terminal block to connect the Edge Gateway to a 8-24V DC power source - please consider “EMC compliant electrical Installation” part in chapter “Intended Use and IT Security Instruction”

Pin	Signal
1	DC IN +8~24VIN (EG800)
2	NC
3	GND

7 Power Consumption

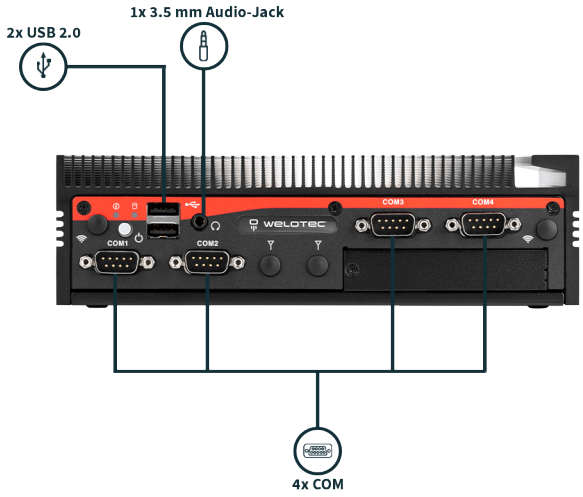
Item	Specification
CPU	11th Gen Intel® Tiger Lake-UP3 Core™ i5-1145G7E – Quad Core, 8MB Cache, up to 4.10 GHz
RAM	16 GB RAM
Operating System	Windows 10 64-bit
Test Program	Burn-in test 9.0 pro, CPU 100%, RAM 40%, Storage 10%
Storage	2.5” 32GB SSD SATA 6Gb/s

Maximum Power Consumption: 39W

Note: Power consumption varies based on configuration and software usage.

8 Interfaces and Connections

8.1 Front I/O



8.2 Rear I/O