Edge Gateway 500 Series

Version:
v1.1.0

Date:
17.11.2025

Contents

1 Copyright

2 Regulatory Compliances

2.1 Complies with the following EU directives

Radio Equipment Directive (2014/53/EU) only applies to devices containing radio module EM05-G.

No	Short Name
2014/35/EU	Low Voltage Directive (LVD)
2014/53/EU	Radio Equipment Directive (RED)
2014/30/EU	Electromagnetic Compatibility (EMC)
2011/65/EU	Restriction of the use of certain hazardous substances in electrical and electronic equipment Directive (RoHS2)
2015/863/EU	Amendment to Annex II in Directive 2011/65/EU regards the list of restricted substances (RoHS3)

2.2 References of standards applied

Standard	Reference	Issue
EN 18031-1	Common security requirements for radio equipment - Part 1: Internet connected radio equipment	2024
EN 55032	Electromagnetic compatibility of multimedia equipment - Emission Requirements	2015+AC:2016
EN 55035	Electromagnetic compatibility of multimedia equipment - Immunity requirements	2017
EN 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions	2014
EN 61000-3-3	Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems	2013
EN 61000-4-2	Electromagnetic compatibility (EMC). Testing and measurement techniques. Electrostatic discharge immunity test	2009
EN 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test	2006+A1:2008+A2:2010
EN 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4 : Testing and measurement techniques - Electrical fast transient/burst immunity test	2012
EN 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test	2014+A1:2017
EN 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields	2014+AC:2015
EN 61000-4-8	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test	2010
EN IEC 61000-4-11	Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests	2004+A1:2017
EN 301 489-1 (module)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements; Harmonised Standard for ElectroMagnetic Compatibility	V2.2.3
EN 301 489-52 (module)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 52: Specific conditions for Cellular Communication User Equipment (UE) radio and ancillary equipment; Harmonised Standard for ElectroMagnetic Compatibility	V1.2.1
Draft EN 301 489-19 (module)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services - Part 19: Specific conditions for Receive Only Mobile Earth Stations (ROMES) operating in the 1,5 GHz band providing data communications and GNSS receivers operating in the RNSS band (ROGNSS) providing positioning, navigation and timing data	V2.2.0
ETSI EN 301 908-1 (mod- ule)	IMT cellular networks; Harmonised Standard for access to radio spectrum; Part 1: Introduction and common requirements Release 15	V15.1.1

2.3 FCC PART 15 VERIFICATION STATEMENT

WARNING

This equipment has been tested and found to comply with the limits for a Class A 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.

May Contain transmitter module:

- XMR2021EM05G

2.4 ICES-003 ISSUE 7 VERIFICATION STATEMENT

CAN ICES3(A)/NMB3(A)

This device complies with CAN ICES-003 Issue 7 Class A. 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. Cet appareil est conforme à la norme CAN ICES-003 Issue 7 Class A. Le fonctionnement est soumis auxdeux conditions suivantes : (1) cet appareil ne doit pas causer d'interférences nuisibles et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant opération indésirable.

May Contain transmitter module:

- 10224A-2021EM05G

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	Comment	Service
LAN 1 … 3		SSH
COM 1	not available in EG400 Mk2	CLI
USB 1 … 4	only 1 interface in 4GB Version	n/a
HDMI	not available in 4GB Version	CLI
DI / GND	not available in 4GB Version	n/a
DO / GND	not available in 4GB Version	n/a
SW / GND	Power Switch	n/a

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 12V 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.

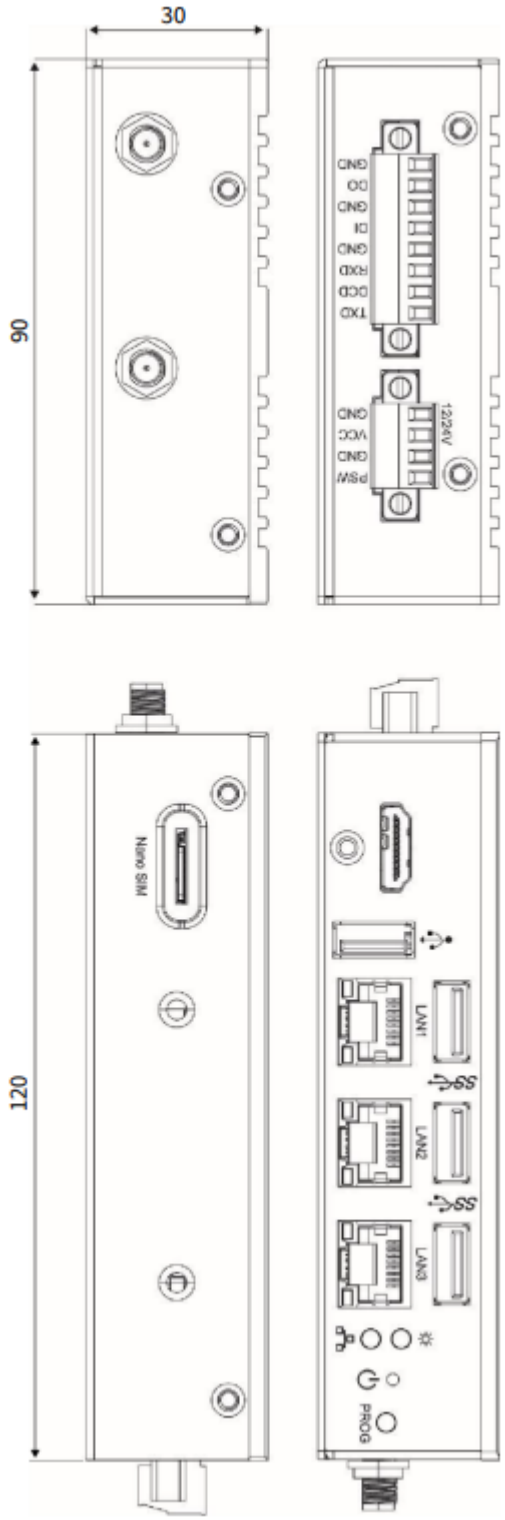
5 Product Specifications

5.1 Technical Details

Feature	Specification	EG503 (4GB RAM)	EG503 (Standard)
Processor	CPU	Intel® Atom™ x5-E3930	Intel® Atom™ x5-E3940
Memory	RAM	4 GB LP-DDR3	8 GB LP-DDR3
Storage	Free Storage	100 GB	100 GB
Security	TPM	TPM 2.0 with TrEE 1.1	TPM 2.0 with TrEE 1.1
I/O Ports	HDMI	-	1
	Gigabit Ethernet	3x RJ45	3x RJ45
	USB 3.0	1	3
	USB 2.0	-	1
	Serial Ports	-	1 RS232 (RS485 optional) (TX/RX only)
	DIO	-	1 DI, 12-24V 1 DO, 12-24V, max. 2 A, output voltage defined by DC input
Connectivity	LTE (EG503L only)	4G	4G
Expansion	SIM Slot	1 push-push Type Nano-SIM Slot	1 push-push Type Nano-SIM Slot
Additional	Watchdog Timer	System Reset, Programmable via Software from 1 to 255 Seconds	System Reset, Programmable via Software from 1 to 255 Seconds
Environmental	Operating Temperature	-20° to 60° C	-20° to 60° C
	Storage Temperature	-20° to 80° C	-20° to 80° C
	Humidity	5% to 95% non-condensing	5% to 95% non-condensing
	IP rating	IP20	IP20
Power	Supply	12 - 24 V DC (+/-10 % tolerance)	12 - 24 V DC (+/-10 % tolerance)
	Connector	Terminal block	Terminal block
Mounting	Options	DIN-Rail	DIN-Rail
Operating System	Compatibility	Welotec egOS	Welotec egOS
Physical Build	Material/Color	Steel / Aluminum	Steel / Aluminum
	Dimensions	130 x 90 x 30 mm	130 x 90 x 30 mm
	Weight	500 g	500 g

5.2 Dimensions

5.2.1 System Drawings



6 Power Supply

 Please ensure no external voltage is applied to PSW! This could cause damage.

Use the terminal block to connect the Edge Gateway to a 12-24V DC power source - please consider “EMC compliant electrical Installation” part in chapter “Intended Use and IT Security Instruction”

Pin	Description
Pin 0 – PSW	External power switch
Pin 1 – GND	Ground
Pin 2 – VCC	V+ 12-24V
Pin 3 – GND	Ground

7 Power Consumption

Item	Specification
CPU	Intel Atom® x5-E3940 Processor
RAM	LP-DDR3 8GB
Operating System	Windows 10 IoT 2021 LTSC
Test Program	3DMark06
Storage	128GB M.2 NVMe

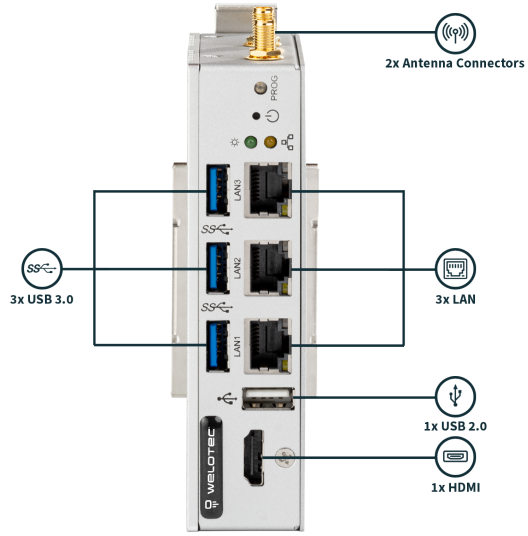
Note: The following results are for reference only.

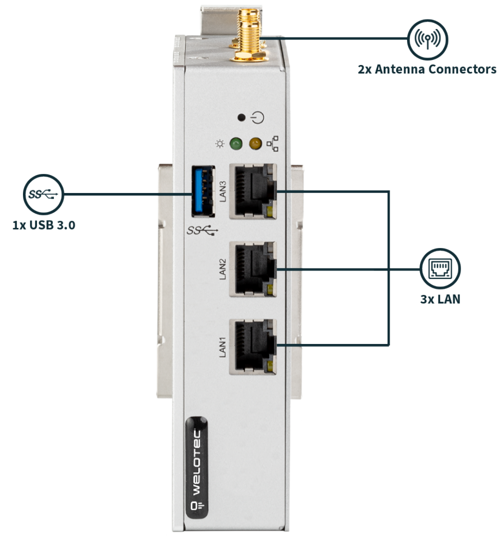
Voltage	Power Off	Startup Max	Startup Stable	EG503W Burn-in Max	EG503L Burn-in Max	Shutdown
12V	0.14A	0.95A	0.62A	1.10A	1.50A	0.82A
24V	0.09A	0.50A	0.32A	0.57A	0.77A	0.42A

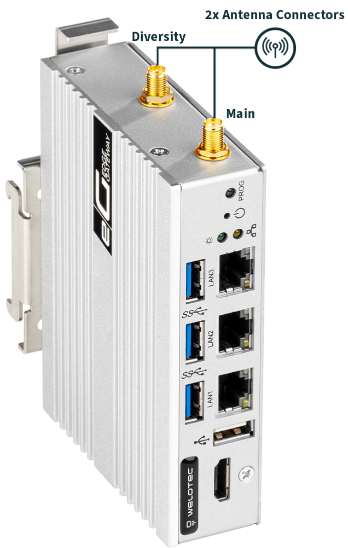
Note: Power consumption varies based on configuration and software usage.

8 Interfaces and Connections

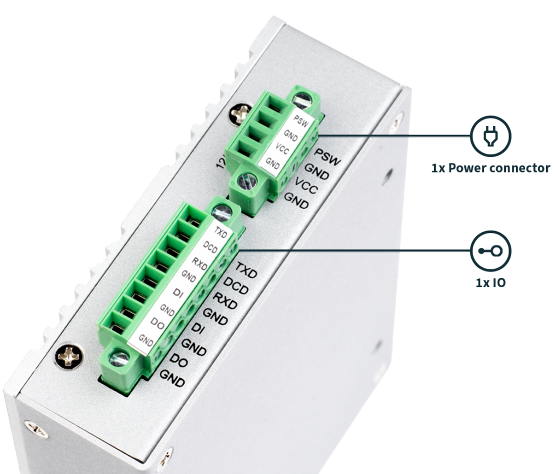
8.1 EG 503L

<table>
<tr><th>EG 503L 8GB</th><th>EG 503L 4GB</th></tr>
<tr><td>


</td><td>


</td></tr>
<tr><td>


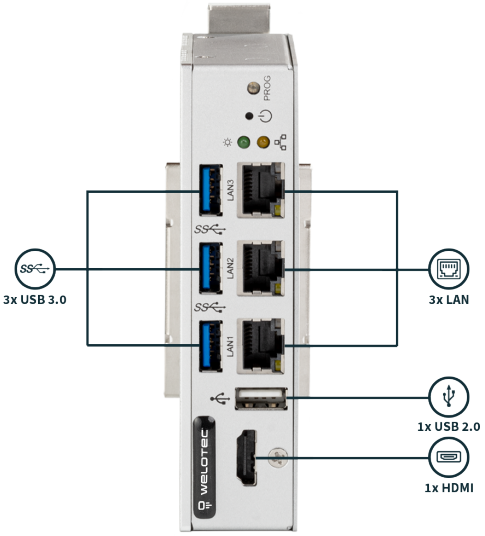
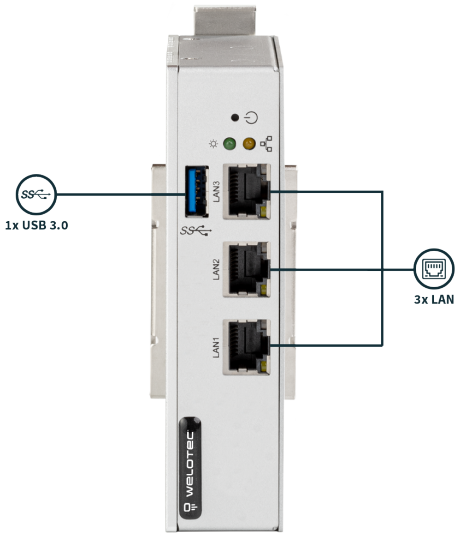
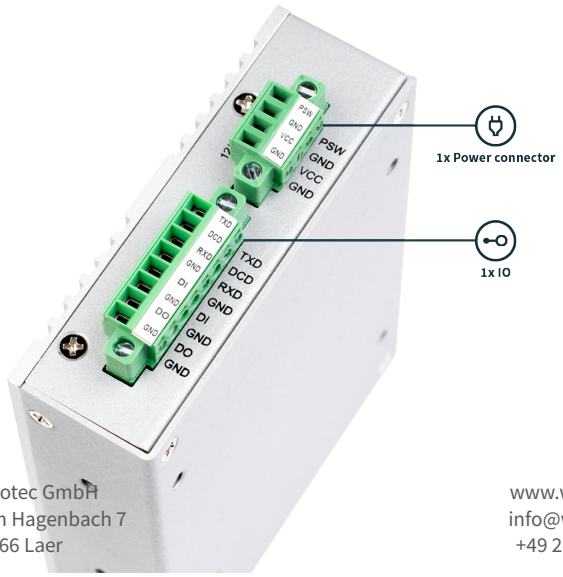
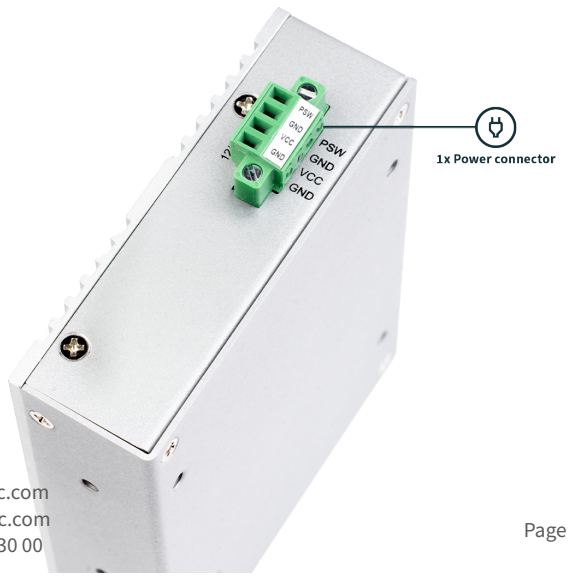
</td><td>


</td></tr>
<tr><td>


</td><td>


</td></tr>
</table>

8.2 EG 503W

EG 503W 8GB	EG 503W 4GB
	
	
	

9 Radio Modules (only relevant with optional LTE/WiFi Modules)

The EG503L may contain the following RF Module:

- Quectel EM05-G

LTE:

Quectel EM05-G	Supported Bands
LTE	FDD B1/ B2/ B3/ B4/ B5/ B7/B8/ B12/B13/B14/ B18/ B19/B20/ B25/ B26/ B28/B66/B71TDD B38/ B39/ B40/ B41
WCDMA	B1/ B2/ B4/ B5/ B6/ B8/ B19

9.1 Radio Frequencies

9.1.1 4G LTE Europe

Band	Frequency Range Down	Frequency Range Up	Max Transmission Power
Band 1	2110 MHz - 2170 MHz	1920 MHz - 1980 MHz	199 mW
Band 3	1805 MHz - 1880 MHz	1710 MHz - 1785 MHz	199 mW
Band 7	2620 MHz - 2690 MHz	2500 MHz - 2570 MHz	199 mW
Band 8	925 MHz - 960 MHz	880 MHz - 915 MHz	199 mW
Band 20	791 MHz - 821 MHz	832 MHz - 862 MHz	199 mW
Band 28	758 MHz - 803 MHz	703 MHz - 748 MHz	199 mW
Band 38	2570 MHz - 2620 MHz	2570 MHz - 2620 MHz	199 mW
Band 41	2496 MHz - 2690 MHz	2496 MHz - 2690 MHz	199 mW

9.1.2 3G UMTS Europe

Band	Frequency Range Down	Frequency Range Up	Max Transmission Power
Band 1	2110 MHz - 2170 MHz	1920 MHz - 1980 MHz	251 mW
Band 8	925 MHz - 960 MHz	880 MHz - 915 MHz	251 mW

Notes

- **Down:** Refers to the downlink frequency range.
- **Up:** Refers to the uplink frequency range.
- **Max Transmission Power:** Maximum power at which the device transmits.