



MOROS.neo

Installation and User Manual

Copyright © July 2026 INSYS icom GmbH

Any duplication of this manual is prohibited. All rights on this documentation and the devices are with INSYS icom GmbH Regensburg.

Trademarks and logos

The use of a trademark or logo not shown below does not indicate that it is freely available for use.

INSYS® is a registered trademark of INSYS MICROELECTRONICS GmbH.

Windows™ is a registered trademark of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

Publisher:

INSYS icom GmbH

Hermann-Köhl-Str. 22

93049 Regensburg

Phone: +49 941 58692 0

Fax: +49 941 58692 45

E-mail: info@insys-icom.com

Internet: <https://www.insys-icom.com>

Date: Jul-26

Item: 10026078

Version: 1.0

Language: EN

1	General	6
1.1	Defects Liability Terms	6
1.2	Applicability	6
1.3	Feedback	6
1.4	Marking of Warnings and Notes	7
1.5	Meaning of the Symbols and the Formatting in this Manual	8
2	Safety Instructions	9
2.1	Intended Purpose	9
2.2	Permissible Technical Limits.....	10
2.3	SIM Card Requirements	10
2.4	Responsibilities of the Operator.....	10
2.5	Qualification of the Personnel.....	10
2.6	Instructions for Transport and Storage	10
2.7	Markings on the Product.....	11
2.8	Protection of the Environment.....	12
2.9	Safety Instructions for Electrical Installation	12
2.10	General Safety Instructions.....	13
3	IT Security.....	15
4	Using Open Source Software	16
4.1	General	16
4.2	Special Liability Regulations	17
4.3	Used Open-Source Software	17
5	Version History	18
6	Device Variants	19
7	Scope of Delivery	20
8	Technical Information	21
8.1	Technical Data	21
8.1.1	Physical Features.....	21
8.1.2	Technological Features.....	23
8.2	Connections, display and control elements.....	24
8.2.1	Display Elements	27
8.2.2	Control Elements	29
8.2.3	Inserting SIM cards	29
8.2.4	Digital inputs/outputs	29
8.2.5	Antennas	31
8.3	Connecting the connectors	32
8.4	Maximum line lengths.....	33
8.5	Certifications	33

9	Mounting	34
10	Commissioning	38
11	Operating Principle	41
11.1	Operation via the user interface.....	42
11.2	Access via HTTPS Protocol.....	44
11.2.1	Authentication via the device-individual certificate/key combination	44
11.2.2	Authentication via an own certificate structure	45
11.3	Profiles and Profile Handling	46
11.4	Term definitions	46
11.4.1	Working with one profile.....	46
11.4.2	Using several profiles	46
11.4.3	ASCII Configuration.....	49
11.4.4	Profile Mode	49
12	Maintenance, Troubleshooting and Repair	50
12.1	Maintenance	50
12.2	Troubleshooting	50
12.3	Repair	50
13	Waste Disposal	51
13.1	Repurchasing of legacy systems	51
14	Declaration of Conformity	52
15	FCC Statement.....	53
16	Export Restriction	54
17	Glossary.....	55
18	Tables and Diagrams.....	58
18.1	List of Tables.....	58
18.2	List of Diagrams	58
19	Index.....	59

1 General

This manual allows for the safe and efficient use of the product. The manual is part of the product and must always be stored accessible for installation, commissioning and operating personnel.

1.1 Defects Liability Terms

A usage not according to the intended purpose, an ignorance of this documentation, the use of insufficiently qualified personnel as well as unauthorised modifications exclude the liability of the manufacturer for damages resulting from this. The liability of the manufacturer ceases to exist.

The regulations of our Delivery and Purchasing Conditions are effective. These can be found on our website (www.insys-icom.com/imprint/) under "General Terms and Conditions".

1.2 Applicability

This manual applies to the product with latest hardware and firmware revision at the time of publication.

1.3 Feedback

We are permanently improving our products and the associated technical documentation. Your feedback is very helpful for this. Please tell us what you like in particular about our products and publications and what can be improved from your point of view. We highly appreciate your suggestions and will include them in our work to support you and all our customers. We are looking forward to any of your feedback.

Send an e-mail to support@insys-icom.de.

We'd like to know your applications. Please send us a few headwords that we know the applications you solve using products of INSYS icom.

1.4 Marking of Warnings and Notes

Symbols and Key Words

Danger!



Risk of severe or fatal injury

One of this symbols in conjunction with the key word Danger indicates an imminent danger. It will cause death or severe injuries if not avoided.



Warning!



Risk of severe or fatal injury possible

This symbol in conjunction with the key word Warning indicates a possibly hazardous situation. It might cause death or severe injuries if not avoid.

Caution!



Slight injury and / or material damage

This symbol in conjunction with the key word Caution indicates a possibly hazardous or harmful situation. It might cause slight or minor injuries or a damage of the product or something in its vicinity if not avoided.

Note



Improvement of the application

This symbol in conjunction with the key word Note indicates hints for the user or very useful information. This information helps with installation, set-up and operation of the product to ensure a fault-free operation.

1.5 Meaning of the Symbols and the Formatting in this Manual

This section describes the definition, formatting and symbols used in this manual. The various symbols are meant to help you read and find the information relevant to you. The following text is structured like a typical operating instruction of this manual.

Bold print: The objective. This will tell you what the following steps will result in

After that, there will be a detailed explanation why you could perform the following steps to be able to reach the objective indicated first. You can decide whether the section is relevant for you or not.

→ An arrow will indicate prerequisites which must be fulfilled to be able to process the subsequent steps in a meaningful way. You will also learn which software or which equipment you will need.

1. *One individual action step: This tells you what you need to do at this point. The steps are numbered for better orientation.*

✓ A result which you will receive after performing a step will be marked with a check mark. At this point, you can check if the previous steps were successful.

ⓘ Additional information which you should consider are marked with a circled "i". At this point, we will indicate possible error sources and tell you how to avoid them.

➤ *Alternative results and steps are marked with an arrow. This will tell you how to reach the same results performing different steps, or what you could do if you didn't reach the expected results at this point.*

2 Safety Instructions

The Safety Instructions section provides an overview about the safety instructions, which must be observed for the operation of the product.

The product is constructed according to the currently valid state-of-the-art technology and reliable in operation. It has been checked and left the factory in flawless condition concerning safety. In order to maintain this condition during the service life, the instructions of the valid publications and certificates must be observed and followed.

It is necessary to adhere to the general safety instructions must when operating the product. The descriptions of processes and operation procedures are provided with precise safety instructions in the respective sections in addition to the general safety instructions.

Moreover, the local accident prevention regulations and general safety regulations for the operating conditions of the device are effective.

An optimum protection of the personnel and the environment from hazards as well as a safe and fault-free operation of the product is only possible if all safety instructions are observed.

2.1 Intended Purpose

The product may be used for the following purposes:

- Usage and installation in an industrial cabinet
- Switching and data transmission functions in machines according to the machine directive 2006/42/EC.
- Usage as data transmission device for a PLC.

The product has no assured properties with regard to functional safety, for example in accordance with the SIL standard. In the event of possible use as a component in a safety function, the system integrator or installer assumes full responsibility for the fulfilment of the safety function.

The product has no assured properties with regard to explosion protection, for example in accordance with the ATEX Directive. In the event of possible use as a component in potentially explosive atmospheres, the system integrator or installer assumes full responsibility for the fulfilment of the scope requirements function.

2.2 Permissible Technical Limits

The product is only intended for the use within the permissible technical limits specified in the data sheets.

The following permissible limits must be observed:

- The ambient temperature limits must not be fallen below or exceeded.
- The supply voltage range must not be fallen below or exceeded.
- The maximum humidity must not be exceeded and condensate formation must be prevented.
- The maximum switching voltage and the maximum switching current load must not be exceeded.
- The maximum input voltage and the maximum input current must not be exceeded.

2.3 SIM Card Requirements

In order to ensure a long function, it is necessary to use so-called M2M SIM cards in industrial quality. Compared to standard SIM cards, industrial SIM cards (also known as M2M or IoT SIM cards) offer not only better mechanical properties but also a significantly longer service life and a much higher number of write cycles, thereby supporting the frequent switching operations that can occur in M2M or IoT applications.

2.4 Responsibilities of the Operator

As a matter of principle, the operator must observe the legal regulations, which are valid in his country, concerning operation, functional test, repair and maintenance of electrical devices.

2.5 Qualification of the Personnel

The installation, commissioning and maintenance of the product must only be performed by trained expert personnel, which has been authorised by the plant operator. The expert personnel must have read and understood this documentation and observe the instructions.

Only a person, who is able to work on electrical installations and identify and avoid possible hazards independently, based on professional training, knowledge and experience as well as knowledge of the relevant standards and regulations is permitted to carry out the electrical connection and commissioning of the product.

2.6 Instructions for Transport and Storage

The following instructions must be observed:

- Do not expose the product to moisture and other potential hazardous environmental conditions (radiation, gases, etc.) during transport and storage. Pack product accordingly.
- Pack product sufficiently to protect it against shocks during transport and storage, e.g. using air-cushioned packing material.

Check product for possible damages, which might have been caused by improper transport and storage, before installation. Transport damages must be noted down to the shipping documents. All claims or damages must be filed immediately and before installation against the carrier or party responsible for the storage.

2.7 Markings on the Product

The identification plate of the product is either a print or a label on a face of the product. Amongst other things, it can contain the following markings, which are explained in detail here.

Observe manual



This symbol indicates that the manual of the product contains essential safety instructions that must be followed implicitly.

Dispose waste electronic equipment environmentally compatible



This symbol indicates that waste electronic equipment must be disposed separately from residual waste via appropriate collecting points. See also Section Disposal in this manual.

CE marking



By applying a CE marking, the manufacturer confirms that the product complies with the European directives that apply product-specific.

UL marking



By applying a UL marking, the manufacturer confirms that the product complies with the obligatory safety requirements.

FCC marking



By applying a FCC marking, the manufacturer confirms that the product complies with the obligatory safety requirements.

Appliance Class II – double insulated



This symbol indicates that the product complies with Appliance Class II

Appliance Class III – protection by extra low voltage



This symbol indicates that the product complies with Appliance Class III

2.8 Protection of the Environment

Dispose the product and the packaging according to the relevant environmental protection regulation. The Waste Disposal section in this manual contains notes about disposing the product. Separate the packaging components of cardboard and paper as well as plastic and deliver them to the respective collection systems for recycling.

2.9 Safety Instructions for Electrical Installation

The electrical connection must only be made by authorised expert personnel according to the wiring diagrams.

The notes to the electrical connection in the manual must be observed. Otherwise, the protection category might be affected.

The safe disconnection of circuits, which are hazardous when touched, is only ensured if the connected devices meet the requirements of VDE 0106 T.101 (Basic requirements for safe disconnection).

The supply lines are to be routed apart from circuits, which are hazardous when touched, or isolated additionally for a safe disconnection.

An easily accessible, fixed installed cut-off device must be installed prior to commissioning to be able to isolate the device from power supply completely (all poles).

2.10 General Safety Instructions

Caution!



Electrostatic discharges may damage the product!

Damage of the product.

Observe the general safety precautions when handling electrostatic-discharge-sensitive parts.

Caution!



Incomplete voltage isolation!

Damage of the product.

To isolate the voltage from the device, disconnect **any** supply circuit with its respective isolation device if a redundant power supply is used.

Caution!



Overcurrent of the device supply!

Fire hazard and damage of the product due to overcurrent.

The product must be secured with a suitable fuse against currents exceeding 3.15 A. It must be ensured that the fuse will only be replaced by a fuse with the same rating in case it needs to be replaced.

Caution!



Moisture and liquids from the environment may seep into the interior of the product!

Fire hazard and damage of the product.

The product must not be used in wet or damp environments, or in the direct vicinity of water. Install the product at a dry location, protected from water spray. Disconnect the power supply before you perform any work on a device which may have been in contact with moisture.

Caution!

Short circuits and damage due to improper repairs and modifications as well as opening of maintenance areas!

Fire hazard and damage of the product.

It is not permitted to open the product for repair or modification exceeding the removal or installation of the designated plug-in cards.

Caution!

Overvoltage and voltage peaks from the mains supply!

Fire hazard and damage of the product due to overvoltage.

Install suitable overvoltage protection.

Caution!

Damage due to chemicals!

Ketones and chlorinated hydrocarbons dissolve the plastic housing and damage the surface of the device.

Never let the device come into contact with ketones (e.g. acetone) or chlorinated hydrocarbons, such as dichloromethane.

Caution!

Distance from antennas to persons!

A too low distance from cellular antennas to persons can affect the health.

Please observe to keep a minimum distance of 20 cm between the cellular antenna and persons during operation.

3 IT Security

Note



Insecure configured routers may compromise security-relevant applications!

Follow the instructions under IT Security Overview to protect your router:

<https://docs.insys-icom.com/docs/en/it-security-en>

For a configuration that meets higher security requirements, a Secure Configuration Guide is also available there (<https://docs.insys-icom.com/docs/en/it-security-secure-configuration-guide-en>).

4 Using Open Source Software

4.1 General

This product contains, amongst others, so-called open-source software that is provided by third parties and has been published for free public use. The open-source software is subject to special open-source software licenses and the copyright of third parties. Basically, each customer can use the open-source software freely in compliance with the licensing terms of the respective producers. The rights of the customer to use the open-source software beyond the purpose of our product are regulated in detail by the respective concerned open-source software licenses. The customer use the open-source software freely, as provided in the respective effective license, beyond the purpose that the open-source software gets in our product. In case there is a contradiction between the licensing terms for our product and the respective open-source software license, the respective relevant open-source software license takes priority over our licensing terms, as far as the respective open-source software is concerned by this.

The use of the used open-source software is possible free of charge. We do not demand usage fees or any comparable fees for the use of the open-source software contained in our product. The use of the open-source software in our product by the customer is not part of the earnings we achieve with the contractual compensation.

All open-source software programs contained in our product can be taken from the available list. The most important open-source software licenses are listed in the Licenses section at the end of this publication.

As far as programs contained in our product are subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Clarified Artistic License or another open-source software license, which regulates that the source code must be made available, and if this software is not already delivered in source code on a data carrier with our product, we will send you this at any time upon request. If it is required to send this on a data carrier, the sending will be made against payment of a cost compensation of € 10,00. Our offer to send the source code upon request ceases automatically 3 years after delivery of our product to the customer. Requests must be directed to the following address, if possible under specification of the serial number:

INSYS icom GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Phone: +49 941 58692 0
Fax: +49 941 58692 45
E-mail: support@insys-icom.de

4.2 Special Liability Regulations

We do not assume any warranty or liability, if the open-source software programs contained in our product are used by the customer in a manner that does not comply any more with the purpose of the contract, which is the basis of the acquisition of our product. This concerns in particular any use of the open-source software programs outside of our product. The warranty and liability regulations that are provided by the respective effective open-source software license for the respective open-source software as listed in the following are effective for the use of the open-source software beyond the purpose of the contract. In particular, we are not liable, if the open-source software in our product or the complete software configuration in our product is changed. The warranty granted with the contract, which is the basis of the acquisition of our product., is only effective for the unchanged open-source software and the unchanged software configuration in our product.

4.3 Used Open-Source Software

You can find a list of the open-source software used in this product by clicking ? > Open-Source Licenses in the title bar of the router's user interface. Alternatively, you can contact our support department (support@insys-icom.de) for a list of the open-source software used in this product.

5 Version History

Version	Modification
1.0	Release

6 Device Variants

This manual describes different variants of the industrial router series MOROS.neo of INSYS icom. The routers are referred to as MOROS.neo in the manual. The routers are:

- MOROS.neo-E (4x 1 GBit/s Ethernet, 2 DI/O, RS-485, Router)
- MOROS.neo-EW (4x 1 GBit/s Ethernet, WiFi, 2 DI/O, RS-485, Router)
- MOROS.neo-E.4G (4x 1 GBit/s Ethernet, 4 DI/O, 1 DI, cellular radio 4G, RS-485, RS-232, Router)
- MOROS.neo-EW.4G (4x 1 GBit/s Ethernet, WiFi, cellular radio 4G, 4 DI/O, 1 DI, RS-485, RS-232, Router)

If the routers are different, this will be mentioned explicitly in the respective sections.

7 Scope of Delivery

The scope of delivery includes all accessories listed below. Please check if all accessories are included in the box. If a part is missing or damaged, please contact your distributor.

- Industrial Routers
 - Top connector
 - Front connector (only MOROS.neo-E.4G and MOROS.neo-EW.4G)
- Quick Installation Guide
- Safety Instructions

The scope of delivery does not include optional accessories. Among other things, the following parts are available from your distributor or INSYS icom:

- WiFi and cellular antennas
- Antenna extensions
- Din rail power supply units
- Device App icom Data Suite
- VPN service
icom Connectivity Suite - VPN
- M2M SIM card and management portal
icom Connectivity Suite - M2M SIM
- Central device management for certificates, updates and configurations
icom Router Management

8 Technical Information

The following information applies to all variants of the router. If these variants differ, the different values will be indicated separately.

8.1 Technical Data

8.1.1 Physical Features

All specified data was measured with nominal input voltage, at full load, and an ambient temperature of 25 °C. The limit value tolerances are subject to the usual variations.

Physical Feature	Value
Operating voltage	12 ... 24 V DC ($\pm 20\%$), protection against reverse polarity and voltage surges (surge/transient)
Power consumption	MOROS.neo-E: typ. 3.5 W, max 5 W MOROS.neo-EW: typ. 3.5 W, max 5 W MOROS.neo-E.4G: typ. 4 W, max 8 W MOROS.neo-EW.4G: typ. 4 W, max 8 W
Level digital input DIO 1/2 (also IO 1/2 for MOROS.neo-E.4G/-EW.4G)	Level HIGH = 2 ... 24 V Level LOW = 0 ... 1 V Contact open condition: HIGH
power consumption input DIO 1/2 at LOW potential (also IO 1/2 for MOROS.neo-E.4G/-EW.4G)	Typ. 5 mA when connecting to GND
Digital output DIO 1/2 (Open Collector), max. load (also IO 1/2 for MOROS.neo-E.4G/-EW.4G)	24 V (DC), 50 mA
Max. voltage drop of digital output DIO 1/2 in condition ON (also IO 1/2 for MOROS.neo-E.4G/-EW.4G)	< 1 V (DC) at 50 mA load
Level digital input DI (only MOROS.neo-E.4G/-EW.4G)	Level HIGH = 10 ... 24 V Level LOW = 0 ... 5 V Contact open condition: LOW
Power consumption input DI at HIGH potential	Max. 5 mA at 24 V DC

Physical Feature	Value
Max. transmission power cellular engine UMTS LTE (only MOROS.neo-E.4G/-EW.4G)	+25.7 dBm +25.7 dBm
WiFi output (only MOROS.neo-EW/-EW.4G)	Max. 100 mW
Real-time clock (RTC) buffer time	Typ. 25 days
Weight	MOROS.neo-E: 180 g MOROS.neo-EW: 185 g MOROS.neo-E.4G: 255 g MOROS.neo-EW.4G: 260 g
Dimensions - width - height - depth Width in DIN rail modules	45 mm 113 mm 94 mm 2,5 TE (DIN modules)
Temperature - operation MOROS.neo-E/-EW MOROS.neo-E.4G/-EW.4G	-30 ... 70 °C (extended 75 °C) -30 ... 65 °C (extended 70 °C) see ⓘ below
Temperature - storage	-30 ... 75 °C
Maximum permissible humidity	95% non-condensing
IP rating	Housing IP30
Environmental conditions	Vibration/Schock as per PLC standard EN 61131-2 und EN 60068-2-6, EN 60068-2-27 Temperature tests as per EN 60068-2-1, EN 60068-2-2, EN 60068-2-14, EN 60068-2-30
MTBF (established for variant MOROS.neo-E.4G; others may vary)	> 645.000 h (25°C), as per standard SN 29500 (according to IEC 61709)

Table 1: MOROS.neo – physical features



Depending on the model, the extended temperature range allows a temporary operation under increased temperatures. Please note that temporary functional limitations may occur in this case.

A temporary reduction of the cellular data rate may occur at increased temperatures, for example. This protects the device from excessive heating and occurs in the event of temporarily increased power requirements, such as high cellular data rates or very unfavorable cellular coverage.

For applications with generally increased power requirements, such as continuous data transmission, the extended upper temperature range

is not suitable; the upper temperature limit of the standard range shall apply.



The following requirements for the external power supply apply to devices that support radio connections (mobile, Wi-Fi):

- PS2 classified as per IEC62368-1
- Short-circuit current < 8 A

8.1.2 Technological Features

Technological Feature	Description
Ethernet port	10/100/1000 Mbit/s full/half duplex auto sense; Auto - MDI/ MDI-X; automatic detection of "crossover" or "patch" wiring.
Isolation voltage	1.5 kV
RS-232 interface (EIA-232)	Max. baud rate 230,400 bit/s; software handshake XON/XOFF; various data formats
RS-485 interface (EIA-485)	Max. baud rate 230,400 bit/s
LTE frequency bands (4G) Band (MHz)	B1 (UL 1920–1980 / DL 2110–2170 MHz) B2 (UL 1850–1910 / DL 1930–1990 MHz) B3 (UL 1710–1785 / DL 1805–1880 MHz) B4 (UL 1710–1755 / DL 2110–2155 MHz) B5 (UL 824–849 / DL 869–894 MHz) B7 (UL 2500–2570 / DL 2620–2690 MHz) B8 (UL 880–915 / DL 925–960 MHz) B12 (UL 699–716 / DL 729–746 MHz) B13 (UL 777–787 / DL 746–756 MHz) B14 (UL 788–798 / DL 758–768 MHz) B18 (UL 815–830 / DL 860–875 MHz) B19 (UL 830–845 / DL 875–890 MHz) B20 (UL 832–862 / DL 791–821 MHz) B25 (UL 1850–1915 / DL 1930–1995 MHz) B26 (UL 814–849 / DL 859–894 MHz) B28 (UL 703–748 / DL 758–803 MHz) B38 (TDD 2570–2620 MHz) B39 (TDD 1880–1920 MHz) B40 (TDD 2300–2400 MHz) B41 (TDD 2496–2690 MHz) B66 (UL 1710–1780 / DL 2110–2200 MHz) B71 (UL 663–698 / DL 617–652 MHz) LTE Cat 4 (DL: 150 Mbit/s, UL: 50 Mbit/s)

UMTS/HSPA frequency bands (3G) Band (MHz)	B1 (UL 1920–1980 / DL 2110–2170 MHz) B2 (UL 1850–1910 / DL 1930–1990 MHz) B4 (UL 1710–1755 / DL 2110–2155 MHz) B5 (UL 824–849 / DL 869–894 MHz) B6 (UL 830–840 / DL 875–885 MHz) B8 (UL 880–915 / DL 925–960 MHz) B19 (UL 830–845 / DL 875–890 MHz) Max. 42 Mbps (DL); max. 5.76 Mbps (UL)
SIM card reader	Dual SIM Single Standby (DSSS); support of 1.8 V and 3.0 V SIM cards Format: Nano-SIM (4FF)
SMS	Dispatch / receipt
Antenna	4G: 2x2 MIMO in downlink direction 3G: Rx Diversity
WiFi	IEEE 802.11 a/b/g/n/ac/ax (Wi-Fi 6), 2.4 and 5 GHz WiFi Station (Client), WiFi AP for up to 16 clients simultaneously, WPA/WPA2/WPA3 (AES, TKIP), 802.1x (EAP, TLS, TTLS, PEAP)

Table 2: MOROS.neo – technological features

- ❗ In practice, the maximum data rates of the wireless interface for LTE Cat 4 are usually impossible to achieve. Among other factors, they are limited by the achievable throughput of the respective Ethernet interface (current reception conditions (network signal strength), the antenna (use of MIMO/Rx diversity, see 8.2.5 Antennas), power and positioning, and support from the respective provider (contract terms and network utilization).
- ❗ The SIM card tray may only be removed when the device is disconnected from the power supply.

8.2 Connections, display and control elements

The following descriptions refer to a maximum equipped variant of the router. Depending on the variant, your router might not provide all connections, display or control elements.

The following image shows the MOROS.neo-E on the left and the MOROS.neo-EW.4G on the right as examples.

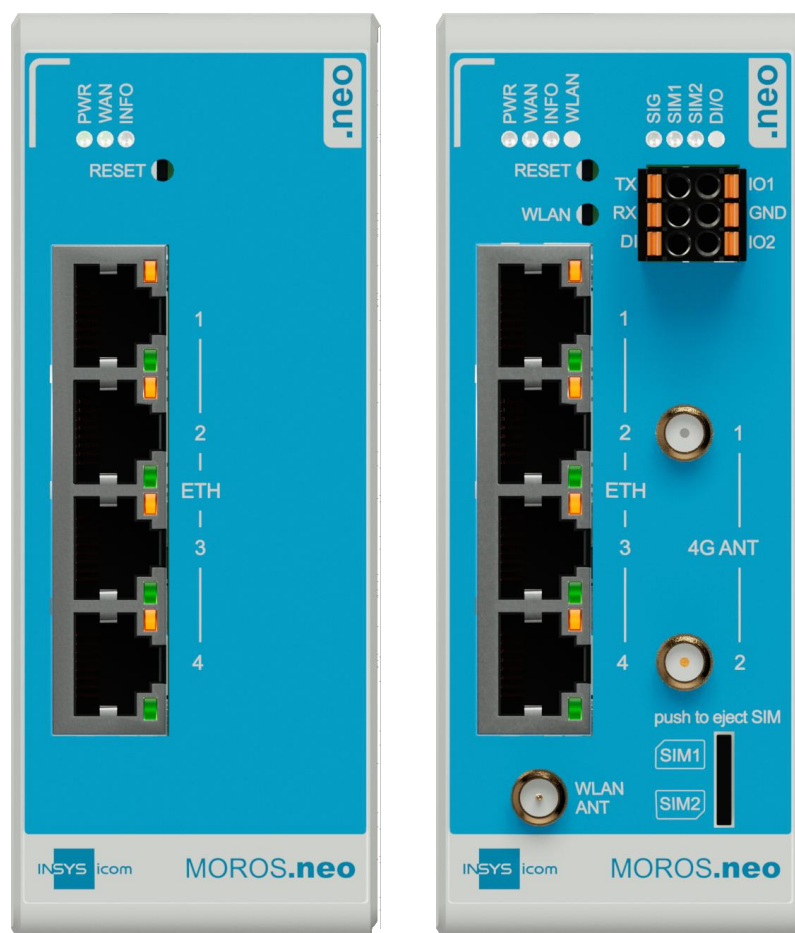


Figure 1: MOROS.neo – Connections, display and control elements

Connection	Description
ETH 1-4	Ethernet port 1 (RJ45, 10/100/1000 BT)
WLAN ANT	WiFi antenna (RP-SMA socket (reverse-polarity)) max. torque of the SMA connector 40 ... 50 Ncm only MOROS.neo-EW/-EW.4G
4G ANT 1	(Primary) cellular antenna 1 (SMA socket) max. torque of the SMA connector 40 ... 50 Ncm only MOROS.neo-E.4G/-EW.4G
4G ANT2	Auxiliary antenna for MIMO / Rx Diversity (SMA socket) max. torque of the SMA connector 40 ... 50 Ncm only MOROS.neo-E.4G/-EW.4G
SIM 1/2	Slot for Nano SIM cards 1 and 2 only MOROS.neo-E.4G/-EW.4G

Table 3: MOROS.neo – front connectors



The screen of the antenna system must be connected to the protective conductor when using an outside mounted antenna.

- ❗ As per EN 2014/53/EU, the operator of a radio equipment must comply with the harmonisation legislation. This includes in particular the selection and utilisation of suitable antenna systems. It must be ensured in particular that devices with radio technology are not operated without a suitable antenna system for an extended period.
- ❗ Do not use WiFi antennas with a gain of more than 3.6 dBi (2.4 GHz) or 4.6 dBi (5 GHz)!

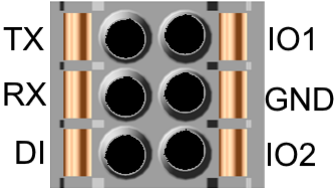
	TX	RS-232 Transmit data line
	RX	RS-232 Receive data line
	DI	Digital input (HIGH active)
	IO1	Digital input/output 1
	GND	Ground, IO and RS-232)
	IO2	Digital input/output 2

Table 4: MOROS.neo-E.4G/-EW.4G – front connectors

	B	RS-485 interface - data line B
	A	RS -485 interface - data line B
	DIO 1	Digital input/output 1
	DIO 2	Digital input/output 2
	GND	Ground (V, IO and RS-232)
	V+	Power supply, positive terminal

Table 5: MOROS.neo – top connector

- ❗ The connection to an AC supply network must be made using a suitable power supply unit.

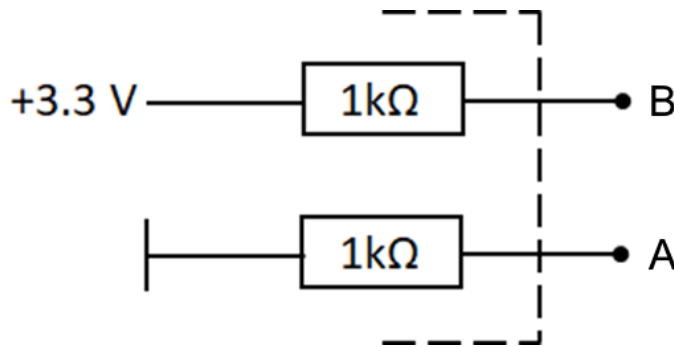


Figure 2: Principle circuit diagram of the RS-485 interface

8.2.1 Display Elements

8.2.1.1 Switch port LED

Each switch port has a green and an orange LED.

The colour indicates the data rate used on the respective port:

- green + orange – 10 Mbps
- only green – 100 Mbps
- only orange – 1000 Mbps

The status of the LED indicates the function:

- off – no data connection (no cable connected, cable defective or network interface on the connected device is not available)
- blinking – data is being transmitted
- on – data connection established, but no data is being transmitted

8.2.1.2 Power LED

The PWR (Power) LED indicates the device status and the boot process.

- off – device powered down
- blinks green – 1x with soft reset, 3x when resetting to default factory settings
- lights green – device is powered on and booted
- lights orange – boot process is running
- blinks red – reset is being performed
- lights red – device has been decommissioned using the 'Secure decommissioning' function and is currently in rescue mode

8.2.1.3 WAN LED

The WAN LED indicates the status of the WAN chain.

- off – WAN chain not active
- blinks green – primary WAN chain is being established
- lights green – primary WAN chain established up to the final interface
- blinks orange – non-primary (alternative) WAN chain is being established
- lights orange – non-primary (alternative) WAN chain established up to the final interface

8.2.1.4 INFO LED

The INFO LED can be individually configured and indicates the following in factory settings.

- blinks **orange** – profile active $\neq$ saved
- lights **red** – boot process is running

8.2.1.5 WLAN LED

The WLAN LED indicates the status of the WiFi interface (only MOROS.neo-EW/-EW.4G).

- off – WiFi disabled or not active
- lights **green** – connection established in station mode, active, and at least 1 client connected in AP mode
- blinks **orange** – active, but no connection established in station mode; active, but no client connected in AP mode

8.2.1.6 SIG LED

The SIG (Signal) LED indicates the signal strength of the cellular connection currently in use (SIM1 or SIM2) (only MOROS.neo-E.4G/-EW.4G).

- off – SIM1 or SIM2 not registered
- blinks **green** – PDN connection established, for signal strength see Table 6
- blinks **orange** – no PDN connection established, for signal strength see Table 6

8.2.1.7 SIM1 LED

The SIM1 LED indicates the status of the SIM card in slot SIM1 (only MOROS.neo-EW/-EW.4G).

- off – no SIM card inserted in SIM1 or SIM card not valid
- lights **green** – SIM card in SIM1 is being used

8.2.1.8 SIM2 LED

The SIM2 LED indicates the status of the SIM card in slot SIM2 (only MOROS.neo-EW/-EW.4G).

- off – no SIM card inserted in SIM2 or SIM card not valid
- lights **green** – SIM card in SIM2 is being used

8.2.1.9 DI/O LED

The DI/O LED indicates a change in the status of a digital input/output (only MOROS.neo-E.4G/-EW.4G).

- blinks **green** – a digital input has changed its state
- blinks **orange** – a digital output has changed its state

Blinking interval LED signal	Signal quality
on	maximum
900 ms on, 100 ms off	very good
200 ms on, 200 ms off	good
100 ms on, 900 ms off	poor
off	no signal or logged out

Table 6: Signal LED blinking cycle

8.2.2 Control Elements

Designation	Operation	Meaning
RESET	Press 1x for 1-3 seconds and release. Power LED blinks 1x green to confirm	Resets the software and restarts it.
	Press briefly three times in quick succession within 3 seconds, or press and hold for at least 8 seconds. Power LED blinks 3x green to confirm	Deletes all settings and resets the device to the factory defaults.

Table 7: MOROS.neo – function and meaning of the control elements

8.2.3 Inserting SIM cards

Gently press the SIM card tray inwards using your fingernail or a small flat-head screwdriver to release the catch, allowing the tray to slide out of the housing slightly. Then pull the tray out completely.

Then insert the Nano-SIM card into the slot on the relevant side of the tray (labelled SIM1/SIM2), with the contacts facing outwards. Please take care to note the bevelled edge.

Then reinsert the SIM card tray into the router and press it gently until you feel it click into place.



The SIM card tray can only be inserted into the device in one orientation. If necessary, turn the tray if it does not slide in easily.

8.2.4 Digital inputs/outputs

The router has two configurable digital inputs/outputs. The digital inputs/outputs are configured as input in default setting.

If the input/output is configured as input, it is low-active, i.e. active, if it is connected to GND.

If the input/output is configured as output, it is designed as open collector output. You'll find more information in Table 1.

The following illustrations show an example of an input connection and two examples of output connections: on the left, an LED; on the right, a relay.

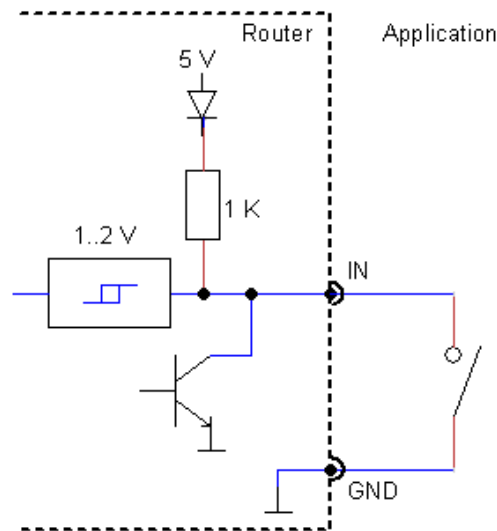


Figure 3: Digital input (low-active) – connection example

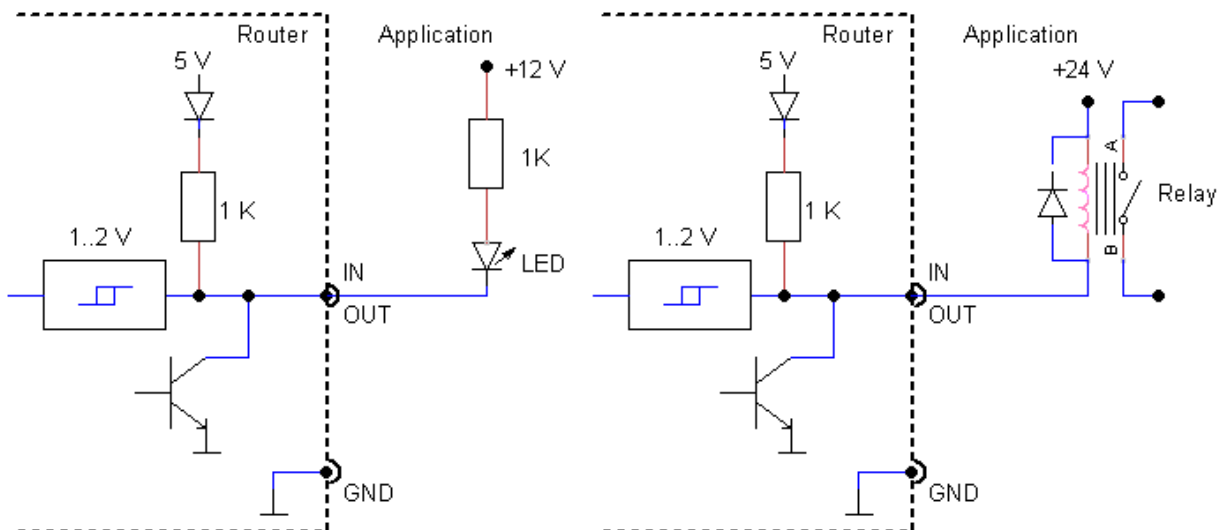


Figure 4: Digital open collector output – connection example

MOROS.neo-e.4G and -EW.4G routers feature two additional configurable digital inputs/outputs and one further digital input.

The digital inputs/outputs IO1 and IO2 correspond to the digital inputs/outputs described above.

The digital input DI is high-active and based on the electrical requirements of the PLC standard DIN EN 61131-2 for digital inputs type 1. You'll find more information in Table 1. The illustration below shows an example of how to connect the input.

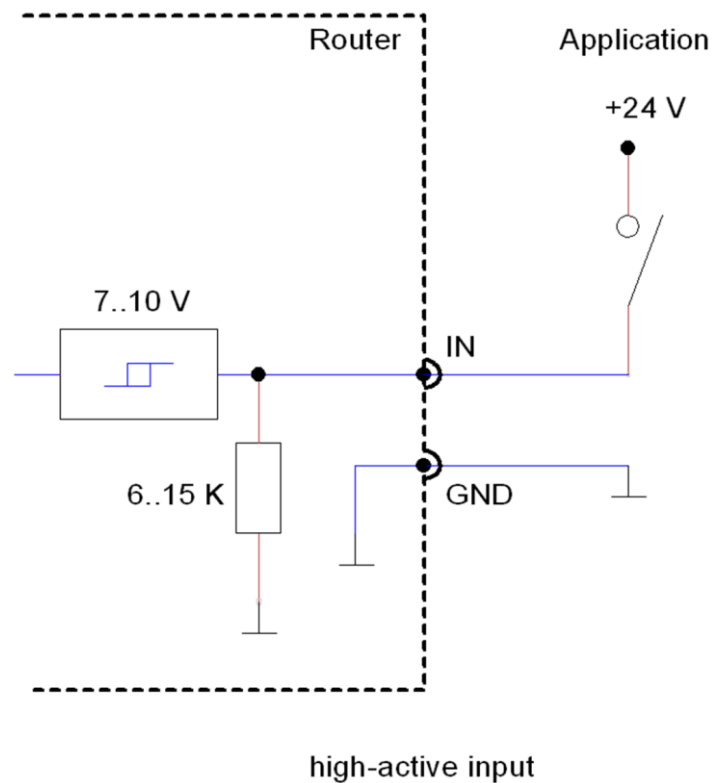


Figure 5: Digital input high-active – connection example

8.2.5 Antennas

- ① As per EN 2014/53/EU, the operator of a radio equipment must comply with the harmonisation legislation. This includes in particular the selection and utilisation of suitable antenna systems. It must be ensured in particular that devices with radio technology are not operated without a suitable antenna system for an extended period.
- ① Separate antennas must be used for mobile networks and WiFi. Combined antennas (mobile and WiFi) must not be used. These separate antennas must be at least 20 cm apart.

In order to meet the respective cellular radio specification (and improve reception quality and data rate in downlink), it is necessary to use a second antenna for the operating modes Rx Diversity (UMTS) or MIMO (LTE) or a MIMO/diversity antenna with two integrated antennas. The following must be observed when using two individual antennas.

8.2.5.1 Main antenna

Since the main antenna is both, first reception antenna and only sending antenna, it should be set-up vertically polarised and omnidirectional to be perfectly aligned with the base station (that is always vertically polarised). It should be possible to compensate the attenuation losses of the antenna lead with an appropriate gain of the antenna.

8.2.5.2 Auxiliary antenna for MIMO / Rx Diversity

When using an auxiliary antenna, it is recommended to use the same type and the same antenna lead as for the main antenna. It would be adverse if the difference in gain of the two antennas is too high. The auxiliary antenna is to be installed at an angle of 90° to receive the horizontally polarised portion of the radio waves that are least “detected” by the main antenna. This allows to compensate negative effects with adverse transmission. Moreover, the possible data rate increases, in particular of the base station broadcasts using two antennas.

8.2.5.3 Antenna arrangement

The distance between the antennas should be as close as possible but not fall below $\frac{1}{4}$ of the maximum wave length (lowest frequency band). Approx. 9 cm would be ideal in case of 800 MHz (LTE, band 20) for example.

Tests have shown that the right arrangement of the antennas is very important. If both antennas are set-up vertically for example, the data rate can be worse than for only one antenna.

8.2.5.4 Outside mounted antenna

When using the outside mounted antennas offered by INSYS, the delivered mounting bracket provides sufficient distance to the wall. If the main antenna is aligned vertically and the auxiliary antenna is mounted at the same point perpendicular, the mounting brackets provide also a minimum distance of the antennas at the feeding point of 10 cm.

8.2.5.5 Magnetic base antenna

The magnetic base antennas offered by INSYS are especially intended for the use on metallic surfaces, e.g. outside a switch cabinet. The metallic, reflecting underground is mandatory for a good antenna effect. Both antennas are to be mounted at an upper corner of the switch cabinet such that the main antenna is on the top of the switch cabinet and the auxiliary antenna on its side wall. The minimum distance at the feeding point must also be observed here.

8.3 Connecting the connectors

The wires are contacted maintenance-free in the connector via a spring clip. Rigid wires (stripped) or stranded wires with end sleeves are only inserted into the connectors to clamp them. Stranded wires (braids) without end sleeve are clamped by pushing in the orange opener (e.g. using a flat-blade screwdriver with max. 3.5 mm width). Unclamping a wires is also done by pushing in the opener.

The permissible wire cross-sections can be found in the following table.

Wire	Cross-section
Nominal cross-section	1.5 mm ²
Rigid	0.2 ... 1.5 mm ²
Flexible	0.2 ... 1.5 mm ²
Flexible with end sleeve without collar	0.25 ... 1.5 mm ²
Flexible with end sleeve with collar	0.25 ... 0.75 mm ²

Table 8: Permissible wire cross-sections for connectors

8.4 Maximum line lengths

The maximum line lengths to the connections can be found in the following table.

Wire	Max. length
Antennas, power supply, serial interfaces, inputs and outputs, other signals	30 m

Table 9: Permissible line lengths

8.5 Certifications

The router provides the following certifications:

- EMC, Emission: EN 61000-6-3, EN 55032 Class B
- EMC, Immunity: EN 61000-6-2, EN 55035
- Product safety: IEC/EN 62368-1
- CE: all EU countries, Albania, Bosnia and Herzegovina, Georgia, Iceland, Liechtenstein, Moldova, Montenegro, North Macedonia, Norway, Switzerland, Serbia, Ukraine, the United Kingdom

In addition, the MOROS.neo-E and MOROS.neo-E.4G models have the following approvals:

- FCC Part 15 Class B: USA
- IC (ISED Canada): Canada

You can find the relevant documents in the Knowledge Base on the product information page.

9 Mounting

This section describes how to mount the MOROS.neo to a DIN rail, connect the power supply and uninstall it again. Observe the instructions in the "Safety" section of this manual, in particular the "Safety Instructions for Electrical Installation" for that purpose unconditionally.

Caution!



Moisture and liquids from the environment may seep into the interior of the device!

Fire hazard and damage of the product.

The device must not be used in wet or damp environments, or in the direct vicinity of water. Install the device at a dry location, protected from water spray. Disconnect the power supply before you perform any work on a device which may have been in contact with moisture.

Caution!



The device could be destroyed if the wrong power supply is used!

If the device is operated with a power supply that supplies a voltage exceeding the permissible operating voltage, it will be destroyed.

Make sure that you use the suitable power supply. Refer to the Technical Data section for the proper voltage range.

Caution!



Risk due to mounting failure!

Injury or malfunction due to falling device.

Make sure you install the device so that the potential drop height is less than two (2) metres. When mounting the product at the end of a DIN rail, ensure that the device cannot move axially by accident (e.g., by using end stops or an equivalent mechanical stop).

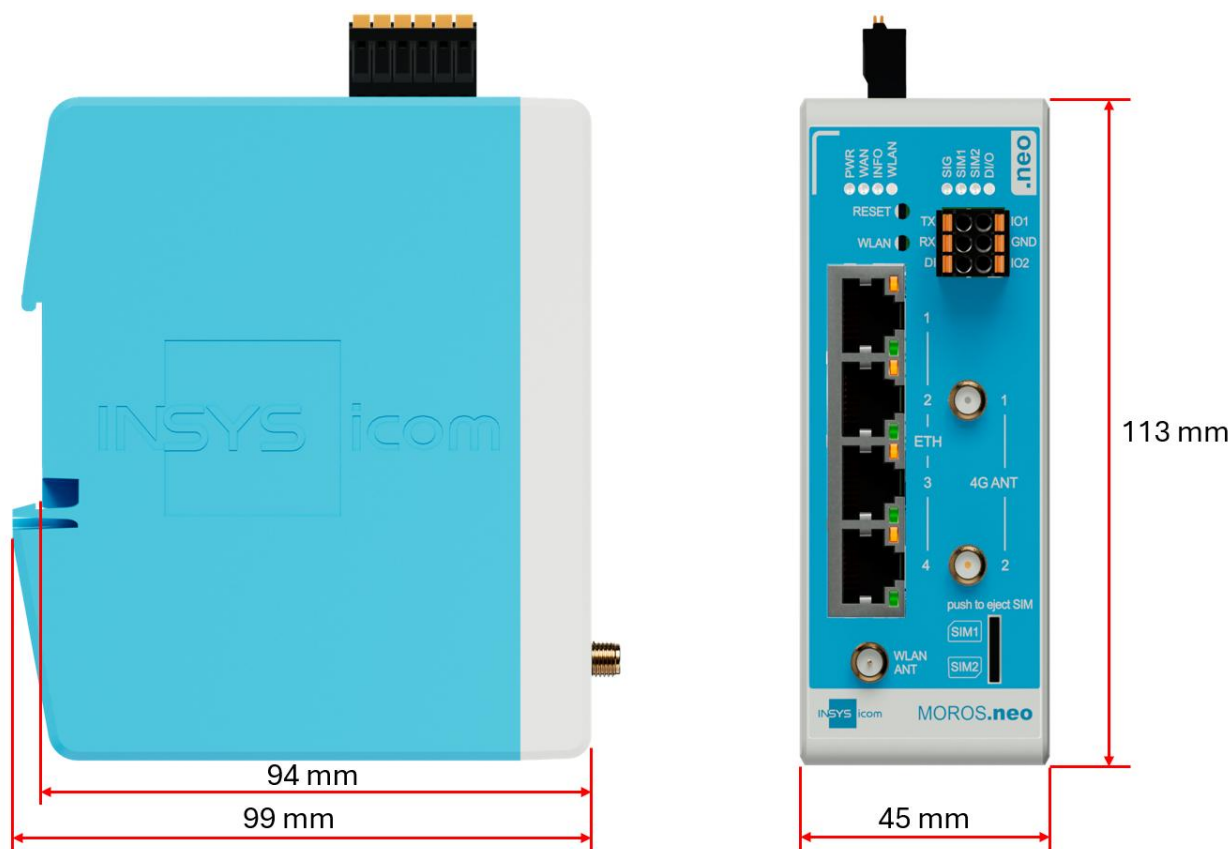


Figure 6: MOROS.neo – dimensions

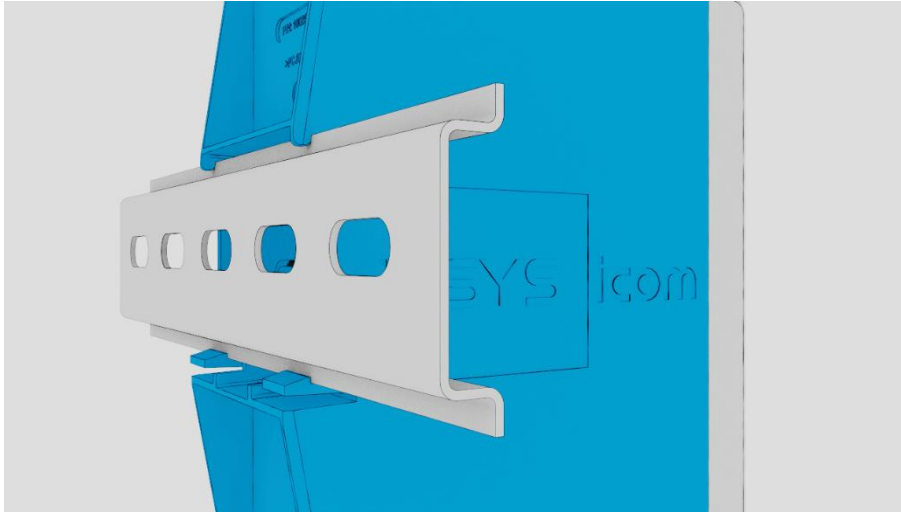
Mounting the device to the DIN rail

How to mount the router to a DIN rail:

1. ***Position the device at the DIN rail as seen in the following diagram. There are two snap-in hooks at the upper DIN rail groove. Hook them into place behind the upper edge of the DIN rail when connecting the device.***



2. ***Fold down the device perpendicular to the DIN rail until the lower, flexible snap-in hooks engage in the DIN rail.***



✓ The router is now readily mounted.

Connecting the power supply

- The device has already been mounted to the DIN rail.
- The power supply is connected and switched off.

1. ***Disconnect the push-in terminal connector at the top of the router.***
2. ***Connect the ground lead of the power supply to the terminal "GND" of the terminal connector.***
3. ***Connect the positive lead of the power supply to the terminal "V+" of the terminal connector.***
4. ***Connect the push-in terminal connector to the terminal strip of the router.***

✓ The router is now connected to the power supply.

Disconnecting the power supply

- The device is mounted to the DIN rail.
- The power supply is connected and switched off.

1. ***Disconnect the push-in terminal connector at the top of the router.***

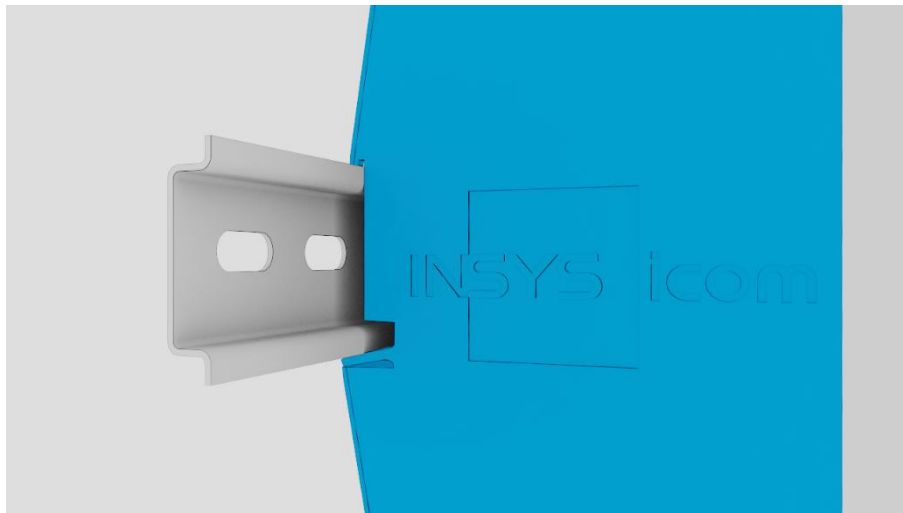
✓ The router is disconnected from the power supply.

Removing the device from the DIN rail

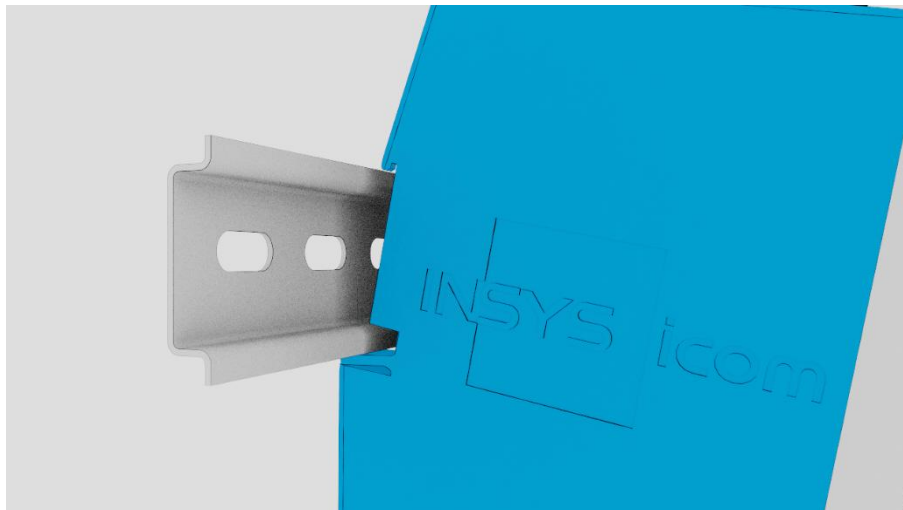
How to uninstall the router from a DIN rail in a switch cabinet:

- The power supply of the switch cabinet is switched off and secured against being switched on accidentally.
- All connectors at the device are disconnected.

- 1. *Push the router vertically upwards on the DIN rail until the upper DIN rail groove is no longer engaged.***



- 2. *Fold down the router away from the DIN rail.***



- ✓ The router is now removed.

10 Commissioning

This chapter describes how to commission the router, i.e. how to connect it via Ethernet to a PC, and how to prepare it for the configuration.

Inserting the SIM card (only MOROS.neo-E.4G/-EW.4G).

How to insert the SIM card (when only using one SIM card).

- The power supply is disabled.
- You will need a functionable Nano-SIM card of your mobile provider.
- You will also need the associated PIN.

1. Gently press the SIM card tray inwards using your fingernail or a small flat-head screwdriver.

✓ The SIM card holder will be ejected a little bit out of the housing.

2. Remove the SIM card holder.

3. Insert your SIM card into the tray in the slot labelled SIM 1.

❗ The SIM card will only fit into the SIM card tray in one position. Note the bevelled edge and make sure that the SIM card does not extend over the card holder.



4. Insert the SIM card holder together with the SIM card again. The contacts of the SIM card must face to the the outside.

5. Using a finger, carefully push the SIM card tray with the inserted SIM card into the housing, until the card holder snaps into place.

6. Enable the power supply again.

Connecting a cellular antenna (only cellular radio version)

How to connect the router to a cellular antenna.

- The power supply is disabled.
- You will need a suitable cellular antenna (available from INSYS icom).

i When selecting and mounting the antenna, make sure to comply with CE conformity. See also the notes under Antennas on page 31.

1. Connect the cellular antenna(s) to the 4G ANT1 and 4G ANT2 antenna sockets.

i If you are using only one antenna, connect it to the 4G ANT1 antenna socket.

✓ The cellular antenna is connected with this.

Connecting a PC

How to connect the router to a PC via a network cable.

- The power supply is disabled.
- You will need a network patch cable (Cat 5e or higher).
- You will need a network card in the PC.

1. Locate the RJ-45 socket of the network card at the PC.

2. Plug one end of the network cable into the RJ45 socket of the PC, and the other end into the ETH 1 socket of the router.

✓ The router is connected to the PC with this.

Configuring the router

- The device is connected to the PC.
- The power supply of the device is enabled and the device is ready for operation (Power LED is illuminated green).
- You have the required access rights to change the IP address of the network card at the PC to which the router is connected in case DHCP cannot be used.

1. Make sure that the DHCP client is enabled for the PC (Obtain an IP address automatically).

i The integrated DHCP server of the router will then allocate an address from the according address range to your network card.

- *Alternatively, you can change the IP address of the network card to which the device is connected to an address that starts with 192.168.1. Do not use the address 192.168.1.1 here. This is the factory default IP address of the device. For example, use 192.168.1.2 as IP address for the network card in your PC.*

2. Open a web browser and enter the host name <https://insys.icom> (or the URL <https://192.168.1.1>) into the address bar.

- ✓ The browser loads the start page of the router.
- *If the browser reports a potential security risk, you can ignore this warning for the initial setup and allow the connection to the router. See also Access via HTTPS Protocol on page 44.*
- *If you see the message in your browser window that the page with this address cannot be found, follow the following steps: Check, whether the device is supplied with power. If yes, most probably a wrong IP address is configured in the device. Press the reset key at least for 8 seconds and repeat this instruction from step 2.*
- ✓ You should now see the start page of the user interface.
- ✓ The router is installed successfully and ready for configuration.

11 Operating Principle

This chapter describes how to operate and configure the router via Ethernet connection.

There are different options for configuration and operation:

- Via a web-based user interface (UI). This is displayed and operated using a web browser. Operation via the UI and access via HTTPS protocol are described in the following.
When you open it for the first time, a landing page appears that leads to the new UI, which replaces the classic web interface and significantly improves the user experience. You can return to the classic view at any time by clicking the button ↶ (to the classic view) in the title bar. The Inline Help in the classic web interface explains the importance of possible settings. It is displayed using the ? button (Display help text) in the title bar besides language selection. An Online Help is available for further explanations that can be opened using links in the Inline Help or the Help -> Documentation menu.
- Via a command line interface (CLI). Configuration and operation via command line are described in detail in the online help in the classic web interface of the router.
- Via a configuration file (binary or ASCII). Configuration and operation via a configuration file are described in detail in the online help in the classic web interface of the router.
- Via the REST interface. Configuration and operation via the REST interface are described in detail in the online help in the classic web interface of the router.

Profiles are used for all types of configuration. The basic handling of these profiles are described at the end of this section.

Note



Insecure configured routers may compromise security-relevant applications!

Follow the instructions in our IT Security Overview to protect your router:

<https://docs.insys-icom.com/docs/en/it-security-hardening-the-router-en>

For a secure initial setup, the router **must** be connected to the computer via a cable since a non-compromisable connection cannot be ensured otherwise.

11.1 Operation via the user interface

The user interface allows easy configuration using a web browser. All functions can be configured via the user interface. The operation is mostly self-explanatory.

- ❗ We recommend using the Startup wizard for the basic configuration of the router.

Access to the user interface

How to access the user interface basically.

- The device is ready for operation and you have access to it (refer to Commissioning section).
- The device is in delivery condition and default settings.

1. ***Start the web browser and enter the host name `https://insys.icom` into the address bar.***

- ❗ The factory default IP address is **192.168.1.1**.
Access is only possible via **HTTPS** protocol in default settings.
If the browser reports a potential security risk, you can ignore this warning for the initial setup and allow the connection to the router.
See also Access via HTTPS Protocol on page 44.

- ✓ The start page of the user interface is displayed.

2. ***Perform the Startup wizard.***

3. ***Make the desired settings and complete the Startup wizard.***

Language selection in the user interface

How to change the language in the user interface.

- The device is ready for operation and you have access to the user interface.

1. ***Click in the title bar on the button and then select the language in the drop-down list .***

- ✓ The user interface is displayed in the selected language then.

Logging out from the user interface

How to log out from the user interface in case an authentication has already been configured and you're logged in to the user interface. This prevents unauthorised access after completing the configuration.

- The device is ready for operation and you have access to the user interface.

1. Click in the title bar on the button and then select the button (Log out).

- ✓ You will be logged out from the user interface and returned to the login screen.

① A session will also be terminated after 15 minutes of inactivity (default setting) due to security reasons.

11.2 Access via HTTPS Protocol

The user interface permits a secure configuration only using the HTTPS protocol in default settings. The HTTPS protocol allows an authentication of the server (i.e. the router) as well as an encryption of the data transmission. It is not recommended to activate the HTTP protocol.

11.2.1 Authentication via the device-individual certificate/key combination

Note



Increased security requirements for critical applications!

Use an Authentication via an own certificate structure for applications with particularly high requirements to security, such as critical infrastructures. Coordinate the proceeding for securing the router with the IT security department of your company.

The following describes an approach that meets common industrial safety levels at all times, taking into account known hazards.

The installation of the CA certificate of INSYS may conflict with the IT security policies of your company.

For a configuration that meets higher security requirements, a Secure Configuration Guide is also available there (<https://docs.insys-icom.com/docs/en/it-security-secure-configuration-guide-en>).

The router is authenticated using a self-signed, device-individual certificate/key combination by default. In case of a first access via the HTTPS protocol, the browser indicates that the router uses an invalid security certificate. The certificate is not trusted, because the CA (certification authority) certificate is unknown. Since the connection to the router is made via a non-compromisable cable connection, you can ignore this warning message and (depending on the browser and operating system) add an exception for this server or establish the secure connection to this server anyway.

11.2.2 Authentication via an own certificate structure

A more secure alternative is to use your own certificate structure and load a self-generated certificate/key combination onto the router and then use this for access via an HTTPS connection.

Proceed as follows in coordination with the IT security department of your company to ensure a secure availability of the router:

1. Ask the DNS administrator of your company to create a DNS entry, which resolves the name of the router (e.g. router01.internal.company-domain.com) to the planned IP address of the router.
2. Ask the PKI administrator of your company responsible for the certificate structure issue and sign a certificate on the name of the router (e.g. router01.internal.company-domain.com).
3. Install this certificate and the associated key on the router as part of a secure initial setup (the router must only be connected to the configuration computer via an Ethernet cable with this). Upload these to the router in the Administration -> Certificates menu.

Select this certificate/key combination in the Administration -> Configuration access -> Web/REST interface menu for the configuration of the Web/REST interface: access via HTTPS.

11.3 Profiles and Profile Handling

The configuration of the router is called profile. Several profiles can be stored on one device so that the configuration of a device can be changed quickly.

11.4 Term definitions

The following terms or conditions are to be distinguished for profiles:

- **running:** the current configuration of the router which is used for operation at the moment
- **opened:** the profile that is currently displayed in the user interface (or CLI or REST interface) for editing
- **last activated, changed:** the last activated profile that differs from the running profile by subsequent changes
- **stored:** one of several possible profiles that are stored on the router by the user

Simple applications do not require the use of more than one profile. However, the router allows many applications by using several profiles. From risk-free testing of modified configurations up to time- or event-triggered switching of different profiles, there are almost no limits for your application.

If the running profile differs from the opened profile, this will be indicated by the appearance of a blinking gear symbol  with the "Activate profile" button.

Following an intentional or unintentional restart of the router (e.g. power supply interruption), the previously running profile will continue to run and the last activated profile will be opened again. If they differ, the button with the gear symbol  blinks again.

11.4.1 Working with one profile

If only one profile is used, the current (opened) profile can be configured in the user interface. Settings made in the opened profile are stored in this profile with a click on the button "Submit" or "OK". They will not become effective in the running profile with this.

If the current profile has been modified, the blinking gear symbol  appears in the title bar. A click on the button with the blinking gear symbol  activates the opened profile, i.e. it becomes the running profile and the modifications of the router configuration become effective. The gear symbol will disappear.



Figure 7: Profile handling – activating

11.4.2 Using several profiles

The versatile possible applications of the router suggest the use of several profiles. The following sections describe the profile handling.

11.4.2.1 Storing a profile

When settings made in the open profile are stored, they will not become effective in the running profile just yet. They become only effective if the opened profile is activated, i.e. made the running profile.

A profile can be stored:

- In the new UI by clicking on the "Submit" button
- In the classic web interface by clicking on the "OK" button

11.4.2.2 Activating a profile

A click on the button with the blinking gear symbol  in the title bar activates the opened profile, i.e. it becomes the running profile.

A stored profile can be activated and opened:

- In the new UI in the "Administration" menu on the "Profiles" page by clicking the  (Edit) button of the respective profile, then on  (activate and open) and "Submit"
- In the classic web interface in the "Administration" menu on the "Profiles" page by clicking on the button with the gear symbol  behind the respective profile.

 If the router is still in default settings, a changed profile cannot be activated until an authentication has been configured.

11.4.2.3 Opening a profile for editing

A stored profile can be opened:

- In the new UI in the "Administration" menu on the "Profiles" page by clicking the  (Edit) button of the respective profile, then on  (open for editing) and "Submit"
- In the classic web interface in the "Administration" menu on the "Profiles" page by clicking on the button with the gear symbol  behind the respective profile.

11.4.2.4 Creating a profile

A new profile can be created from:

- the running profile
- stored profiles
- the default settings

A new profile can be created:

- In the new UI in the "Administration" menu on the "Profiles" page by clicking the  (Add) button and selecting "Create new profile"
- In the classic web interface in the "Administration" menu on the "Profiles" page by making the correspondent selection behind "Create profile from"

The new profile will be created and appears in the list of profiles. The profile can then be given a descriptive name. It must first be opened to edit it.

11.4.2.5 Exporting a profile

Profiles stored on the router can be exported to the computer, i.e. downloaded.

A stored profile can be exported:

- In the new UI in the "Administration" menu on the "Profiles" page by clicking the  (Edit) button of the respective profile
- In the classic web interface in the "Administration" menu on the "Profiles" page behind the respective profile

A click on the button for the binary file download  downloads the profile as a binary file. This is recommended to archive the profile or transmit it to another router, e.g. a backup device.

A click on the button for the ASCII file download  downloads the profile as a ASCII configuration file. This is recommended if the profile is to be edited manually on the computer.

11.4.2.6 Importing a profile or an ASCII configuration file

Profiles (in binary format) or ASCII configuration files can be uploaded to the router.

A profile or an ASCII configuration file can be imported:

- In the new UI in the "Administration" menu on the "Profiles" page by clicking the  (Add) button in the "Profile" section and selecting "Upload profile" or by clicking the  (Upload) button in the "ASCII configuration" section
- In the classic web interface in the "Administration" menu on the "Profiles" page under "Import profile or ASCII configuration file"

The profile or ASCII configuration file will be uploaded and appear in the respective list.

11.4.2.7 Deleting a profile

A stored profile can also be deleted again.

A stored profile can be deleted:

- In the new UI in the "Administration" menu on the "Profiles" page by clicking the  (Edit) button of the respective profile and a click on  (Delete)
- In the classic web interface in the "Administration" menu on the "Profiles" page by clicking on the button with the bin symbol  behind the respective profile

11.4.2.8 Comparing two profiles

To show the differences between two profiles, it is possible to compare the default settings, the running profile and the stored profiles to each other.

For this, you need to select the two profiles to be compared in the "Administration" menu on the "Profiles" page under "Compare profiles". The different settings of both profiles are displayed side by side when clicking the button "OK". This function is currently only available in the classic web interface.

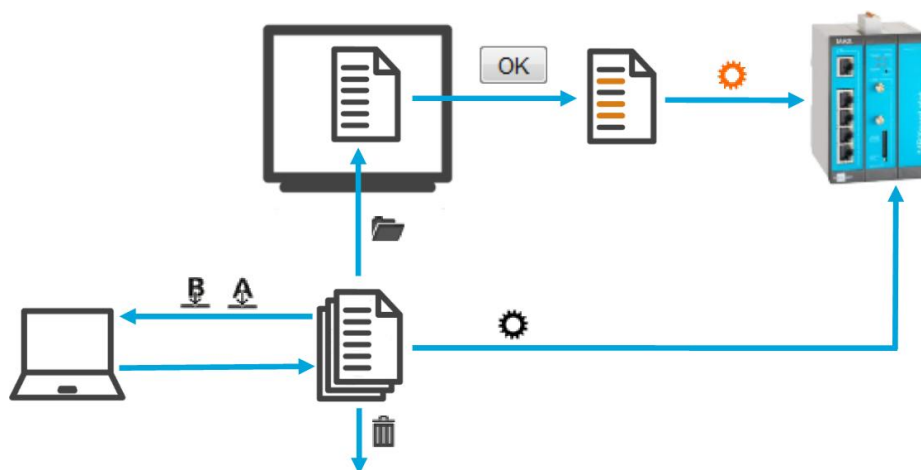


Figure 8: Profile handling – scheme

11.4.3 ASCII Configuration

ASCII configurations are a sequence of commands as they could also be entered in the CLI. Each line contains a command that modifies the opened profile.

Syntax and parameters can be taken from a downloaded profile in ASCII format for example. Refer to the CLI description for further information about the syntax.

Commands that affect plug-in cards that are not installed will be taken over to the profile, but will have no effect.

11.4.4 Profile Mode

The router provides two profile modes: permanent and volatile. The configuration of this function is currently only available in the classic web interface.

The router is in permanent profile mode in normal operation. All modifications are permanently saved and remain intact after a restart.

In certain safety-critical applications, it is required that a router always starts up in a defined basic state after a restart and receives its specific configuration via an update server or router management. A volatile profile mode is available for such purposes. In this mode, all changes to the configuration (including profiles and ASCII configuration files) are lost when the router is restarted and the router restarts in the state it was in when it was changed to volatile mode.

12 Maintenance, Troubleshooting and Repair

12.1 Maintenance

The product is maintenance-free and does not require special regular maintenance.

12.2 Troubleshooting

If a failure occurs during the operation of the product, you will find troubleshooting tips on our support page (<https://www.insys-icom.com/en/support/>). If you need further support, please contact your sales partner or INSYS icom support. You can contact our support department via e-mail under support@insys-icom.de.

12.3 Repair

Information for proceeding in case of repair or complaints are available on our support page (<https://www.insys-icom.com/en/support/>).

Before dispatching the device:

- Remove any inserted SIM cards.
- Backup the configuration on the device and any other stored data if required.
- Backup any applications running on the device.

Caution!



Short circuits and damage due to improper repairs and modifications of products.

Fire hazard and damage of the product.

It is not permitted to open the product for repair or modification.

13 Waste Disposal

13.1 Repurchasing of legacy systems

According to the new WEEE guidelines, the repurchasing and recycling of INSYS legacy devices for our clients is regulated as follows:

Please contact your sales representative by e-mail or phone to initiate a return shipment to INSYS icom.

E-mail: info@insys-icom.de

Phone: +49 941 58692-0



Please consider possible stored passwords or security certificates before disposing the device. It is recommended to block possible existing access rights for the device (e.g. on your VPN server) and reset the device to default settings (if possible), before passing it on or disposing it.

14 Declaration of Conformity

Hereby, INSYS icom GmbH declares that the device type MOROS.neo is in compliance with Directives 2014/53/EU and 2011/65/EU. The full text of the EC Declaration of Conformity is available under the following Internet address:

www.insys-icom.com/manual

To ensure that radio equipment complies with CE requirements, exposure of persons to electromagnetic fields must be limited and therefore checked in relation to the antennas used. Compliance with these requirements can only be guaranteed if the antennas supplied by INSYS as accessory products are used.

If this radio equipment product is incorporated into a non-radio equipment product in accordance with the installation instructions in this manual, a re-assessment of the conformity of the complete product in accordance with the Radio Equipment Directive 2014/53/EU is not required, provided that the product into which this radio equipment product is incorporated is subject to assessment criteria comparable to those of this radio equipment product.

Provided that the combined product does not require a further conformity assessment under Directive 2014/53/EU in accordance with the above requirements, the declaration of conformity for the radio equipment may be used for its declaration of conformity, provided that

- the overall product is subject to equivalent assessment criteria, and
- no changes are made to the radio equipment product.

The above information is a summary of the relevant points of the ETSI EG 203 367 application guideline for the harmonised standards relating to Articles 3.1b and 3.2 of the Radio Equipment Directive 2014/53/EU (RED) for multi-purpose radio equipment and combined radio and non-radio equipment; the content of the guideline takes precedence.

In addition, IT security requirements also apply to system integrators and operators of radio equipment in accordance with the RED. The system integrator or operator must, among other things, ensure that radio equipment is protected against unauthorised access and does not have any known vulnerabilities to cyber attacks, for example by securing communication interfaces. The system integrator or operator is required to ensure that the firmware is updated regularly (see <https://icom-os.releasenotes.io/>), to keep themselves informed about potential security vulnerabilities (see <https://www.insys-icom.com/en/support/security-advisories/>) and to configure the devices (including any container applications that may be installed) in a manner that ensures appropriate IT security (see <https://docs.insys-icom.com/docs/en/it-security-en>).

15 FCC Statement

Note: Certain variants of this device comply with part 15 of the FCC Rules (this is indicated by the FCC symbol on the label). 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.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

16 Export Restriction

The chip sets for analogue modems and cellular radio adapters used by INSYS icom GmbH are subject to export restrictions as per US ECCN classification (5A991).

Therefore, it is not allowed to export these communication devices into the following countries (at the time when this publication has been issued): Cuba, Iran, North Korea, Sudan, Syria

The currently effective country list can be found in section „Country Group E“ in the document "Supplement No. 1 to Part 740" of the Export Administration Regulations (EAR) (<https://www.bis.doc.gov>). Please contact the US authorities directly for a special permit.

We want to make you aware that the US legislation may have an effect in Germany. Amongst others, it may happen that US companies may be precluded from supplying foreign violators of the EAR on the basis of US legislation.

Note



Export restriction!

Possible violation of export regulations.

This device uses encryption technology and is therefore subject to export control as per German (AL classification 5A002) and European law (EG-DUAL-USE VO 428/2009). The export from Germany requires a permission of the Bundesamt für Wirtschaft und Ausfuhrkontrolle (Federal Office of Economics and Export Control).

This device may contain components with US origin. Possible export conditions as per US law (ECCN classification) will be mentioned explicitly on receipts, if possible, or can always be requested.

17 Glossary

This describes the most important terms and abbreviations of this manual.

- APN:** Access Point Name, computer name that provides cellular subscribers of the GPRS network with Internet access.
- AT command:** Commands to devices such as modems to set up this device.
- Broadcast:** Data packet that is sent to all participants of a network.
- Caller ID:** Phone number transmitted by the caller that can be evaluated by the called device.
- Client:** Device that requests services from another device (server).
- DHCP:** Dynamic Host Configuration Protocol; DHCP servers can dynamically design an IP address and other parameters to DHCP clients on request.
- DNS:** Domain Name System; service used for the translation of domain names into IP addresses.
- Domain name:** The domain is the name of an Internet site (e.g. insys-icom). It consists of the name and an extension (Top Level Domain, e.g. .com), (e.g. insys-icom.com).
- DSSS:** Dual SIM Single Standby refers to a dual-SIM system in which two SIM cards are inserted into a single device, but only one SIM can be connected to the network at a time. To ensure redundancy in the event of a provider change, you can switch between the cards.
- EDGE:** Enhanced Data Rates for GSM Evolution designates a technology for increasing the data rate in GSM cellular networks by introducing an additional modulation process. EDGE enhances GPRS to E-GPRS (Enhanced GPRS) and HSCSD to ECSD.
- Firewall:** Network rules that block in particular data packets to certain sources or destinations.
- Gateway:** This is a machine that works like a router. In contrast to the router, a gateway can also route data packets from different hardware networks.
- GPRS:** General Packet Radio Service; advancement of the -> GSM cellular network to achieve higher data transmission rates.
- GSM:** Global System for Mobile communications; cellular network for voice and data transmission.
- ICMP:** Internet Control Message Protocol; protocol that is often used to control a network. The program "ping" uses ICMP for example.
- Interface:** A network device that can transport IP connections.

- IP address:** Internet Protocol address; The IP address of a device in a network under which it can be accessed. It consists of four bytes and is indicated decimal, (e.g. 192.168.1.1)
- IP net:** An Ethernet-based interface that can become a LAN or a WAN interface.
- LAN:** Local Area Network; a network of computers which are located relatively close to each other.
- LAN interface:** An interface that is assigned to a local network (plant network, machine network, local network); it is connected to a WAN via the router.
- MAC address:** Media Access Control Address. A MAC is a part of an Ethernet interface. Each Ethernet interface has a unique global number, the MAC address.
- Netmask:** Defines a logical group of IP addresses in net address and device addresses.
- Net address:** Consists of the overlap of IP address and netmask. It always ends with "0". The netmask (e.g. 255.255.255.0) is applied in binary form to an IP address (e.g. 192.168.1.1); the still "visible" part of this overlapping (masking) is the net address (here: 192.168.1.0).
- Network rules:** You decide how the different data packets are handled in a network device. You can block or redirect data packets to or from certain network participants for example.
- Port:** (1) Socket at the switch for connecting Ethernet devices.
(2) Part of a socket for data connections
- Port-Forwarding:** Network rules that redirect data packets from certain senders to special recipients of a network.
- PPP:** Point to Point Protocol; a protocol, which connects two machines via a serial line to enable the exchange of TCP/IP packets between those two machines.
- PPPoE:** Point to Point Protocol over Ethernet; a protocol, which connects two devices via an Ethernet line to enable the exchange of TCP/IP packets between those two machines.
- Router:** This is a machine in a network, which is responsible for the incoming data of a protocol to be forwarded to the planned destination or sub network.
- SCN:** Service Center Number, phone number of the computer that accepts short messages (->SMS) via the GSM network and forwards them to the recipients.
- Server:** Device that provides services, e.g. web server, to other devices (client).

SMS:	Short Message Service; short messages can be sent via the GSM cellular network.
Socket:	Data connections that are established using ->TCP or ->UDP use sockets for addressing. A socket consists of an IP address and a port (cf. address: street name and number)
Switch:	A device that can connect several machines with the Ethernet. In contrast to a hub, a switch will "think" by itself, i.e. it can remember the MAC addresses connected to a port and directs the traffic more efficiently to the individual ports.
TCP:	Transmission Control Protocol; a transport protocol to enable data exchange between network devices. It operates "connection-based", i.t. the data transmission is protected.
UDP:	User Datagram Protocol; a transport protocol to enable data exchange between network devices. It operates "without connection", i.t. the data transmission is not protected.
UMTS:	Universal Mobile Telecommunications System stands for the third generation cellular standard (3G) that allows significantly higher data transmission rates (384 kbit/s to 7.2 Mbit/s) than the second generation cellular standard (2G), the GSM standard (9.6 kbit/s to 220 kbit/s).
URL:	Uniform Resource Locator; this is the address used by a service to be found in the web browser. In this manual, an URL is mostly entered as the IP address of the device.
VPN:	Virtual Private Network; logical connections (so-called tunnels) are established via existing unsafe connections. The end points of these connections (tunnel ends) and the devices behind can be considered as an independent logical network. A very high degree of tap- and tamper-resistance can be achieved with the encryption of the data transmission via the tunnels and the previous two-way authentication of the participants at this logical network.
WAN:	Wide Area Network; a network consisting of computers, which are located far away from each other.
WAN group:	Defines a collection of WAN interfaces that can be started or stopped in parallel.
WAN interface:	An interface that serves to connect the local network (or one of the local networks) with a superordinate network.
WAN chain:	Defines a WAN by arranging WAN interfaces or WAN groups in a sequence.

18 Tables and Diagrams

18.1 List of Tables

Table 1: MOROS.neo – physical features	22
Table 2: MOROS.neo – technological features.....	24
Table 3: MOROS.neo – front connectors	25
Table 4: MOROS.neo-E.4G/-EW.4G – front connectors	26
Table 5: MOROS.neo – top connector.....	26
Table 6: Signal LED blinking cycle	29
Table 7: MOROS.neo – function and meaning of the control elements.....	29
Table 8: Permissible wire cross-sections for connectors	33
Table 9: Permissible line lengths	33

18.2 List of Diagrams

Figure 1: MOROS.neo – Connections, display and control elements.....	25
Figure 2: Principle circuit diagram of the RS-485 interface.....	27
Figure 3: Digital input (low-active) – connection example	30
Figure 4: Digital open collector output – connection example.....	30
Figure 5: Digital input high-active – connection example	31
Figure 6: MOROS.neo – dimensions	35
Figure 7: Profile handling – activating configuration modifications	46
Figure 8: Profile handling – scheme	49

19 Index

Access Point Name	55	Ground	26
Accessories	20	GSM	55
Additional Information.....	8	GUI interface	42, 44
Alternative results	8	Housing	14
APN	55	HTTPS	44
Assembly.....	34	Humidity.....	22
AT command.....	55	ICMP	56
Basic Safety Instructions.....	13	INFO LED	28
Blinking interval LED signal.....	29	Input	26
Broadcast	55	Intended purpose	9
Caller ID.....	55	Interface	56
Cellular antenna	25, 39	IP address.....	39, 56
Checkmark	8	IP network	56
CLI	41	IP rating	22
Client	55	IT Security	15, 41
Command line	41	Key word	7
Configuration.....	40, 41	LAN	56
Connection	34	LAN interface	56
Defects Liability Terms.....	6	Legacy devices.....	51
DHCP.....	55	Liquids.....	13, 34
DI/O LED	28	MAC address.....	56
DIN rail	35, 36, 37	Marking	7
DNS.....	55	Modification	14, 50
Domain name.....	55	Moisture	13, 34
DSSS	55	Mounting.....	34
EDGE	55	Net address	56
Electrical Installation	12	Netmask	56
Environment.....	34	Network card.....	39
Environmental conditions.....	13	Network patch cable	39
Ethernet.....	23	Network rules	56
Ethernet port	25	Open-Source	16
Explosive atmosphere	9	Operating voltage.....	21
Firewall.....	55	Operation.....	41
Formattings.....	8	Output	26
Gateway	55	Overvoltage	14
General	6	Overvoltage protection.....	14
GPRS	55	PC.....	39

Permissible limit	10	SIM card	25, 38
Personnel	10	SIM card holder	38
PIN	38	SIM card reader	24
Port	56	SIM Card Requirements	10
Port forwarding	56	SIM1 LED	28
Power consumption	21	SIM2 LED	28
Power Consumption	21	SMA socket	25
Power LED	27	SMS	57
Power supply	39	Socket	57
PPP	56	Surface	14
PPPoE	56	Switch	57
Prerequisites	8	Switch cabinet	37
Protection of the Environment	12	Symbol	7, 8
Qualification	10	TCP	57
Recycling	51	Transmission power	22
Removal	34	Transport	11
Repair	14, 50	UDP	57
Reset key	29	UMTS	57
Responsibilities of the operator	10	URL	57
REST interface	41	Usage	9
Router	57	VPN	57
RS-232	23, 26	WAN	57
RS-485	23, 26	WAN chain	58
SCN	57	WAN group	57
Scope of Delivery	20	WAN interface	58
Security	9	WAN LED	27
Server	57	Water spray	13, 34
Service Center Number	57	WiFi antenna	25
Short-cut	14, 50	WLAN LED	28
Signal LED	28		

