

# picoScan150 Hardening Guide

**SICK**  
Sensor Intelligence.



---

**Described Product**

picoScan150

**Manufacturer**

SICK AG  
Erwin-Sick-Str. 1  
79183 Waldkirch  
Germany

**Legal information**

This work is protected by copyright. Any rights derived from the copyright shall be reserved for SICK AG. Reproduction of this document or parts of this document is only permissible within the limits of the legal determination of Copyright Law. Any modification, abridgment or translation of this document is prohibited without the express written permission of SICK AG.

The trademarks stated in this document are the property of their respective owner.

© SICK AG. Copyright reserved.

**Original document**

This document is an original document of SICK AG.

Content

- 1 About this document ..... 5**
  - 1.1 Further cybersecurity information..... 5
    - 1.1.1 Security Advisories..... 5
    - 1.1.2 Reporting Security Vulnerabilities ..... 5
  - 1.2 Further product information ..... 5
  - 1.3 Legal notice ..... 6
  - 1.4 Liability ..... 6
  
- 2 General recommendations ..... 8**
  - 2.1 Intended use..... 8
  - 2.2 Environmental influences ..... 8
  - 2.3 Physical access restriction..... 8
  - 2.4 Limit exposure to public networks ..... 8
  - 2.5 Elaborate an update strategy ..... 8
  - 2.6 Configuration backup and restore ..... 9
    - 2.6.1 Backup (export)..... 9
    - 2.6.2 Restore (import)..... 9
  - 2.7 Data integrity ..... 10
  - 2.8 Brute-force..... 10
  - 2.9 Periodic test..... 10
  - 2.10 Device Identification ..... 10
  - 2.11 Use Device-Not-Ready status..... 11
  
- 3 Protection Levels ..... 12**
  - 3.1 No protection ..... 12
    - 3.1.1 Set factory default..... 12
  - 3.2 Basic protection..... 14
    - 3.2.1 Check for latest firmware / release notes ..... 14
    - 3.2.2 Change passwords..... 14
    - 3.2.3 Password reset ..... 15
    - 3.2.4 Configure Network Settings ..... 17
    - 3.2.5 Disconnect unused interfaces ..... 17
    - 3.2.6 Close unused ports / services ..... 18
  - 3.3 Advanced protection..... 23
    - 3.3.1 Limit network access (IP-range)..... 23
  
- 4 Application related recommendations ..... 24**
  - 4.1 Primary sensor data..... 24
    - 4.1.1 Measurement data output..... 24
  - 4.2 Secondary sensor data..... 25
    - 4.2.1 IMU data output..... 25
    - 4.2.2 Command ID..... 25
    - 4.2.3 Telegram Version ..... 25

# CONTENT

---

4.2.4	IMU Sensor Timestamp .....	26
4.2.5	CRC32 checksum.....	26
4.4	Recommended Security measures .....	26
4.4.2	Messages .....	26
4.4.3	Diagnostic file.....	27
4.4.4	Changing Parameter.....	27

## 1 About this document

At SICK, Cybersecurity covers the entire product life cycle. The increasing digitalization and growing network complexity of production plants increases the risk of cyberattacks. These attacks can originate inside or outside the production network. For this reason, a comprehensive cybersecurity strategy is essential.

The asset owner is a person or organization responsible for operation and maintenance of a system. The asset owner has the responsibility to install and maintain security measures. Securing SICK devices in a network requires active participation of the asset owner.

This document contains information about security aspects of picoScan150:

- Communication security and access management
- Application (Field evaluation) aspects

This document provides technical advice for anyone involved in deploying picoScan150.

Version of this document: **V1.0.0**

The following points have been considered in relation to cybersecurity

- User level
- USB/ Display
- Device Interfaces
- Application related recommendations
- Ethernet related settings

### 1.1 Further cybersecurity information

For Cybersecurity overview, please refer to SICK Operating Guidelines (8024601), see [www.sick.com/psirt](http://www.sick.com/psirt).

#### 1.1.1 Security Advisories

SICK takes security very seriously and our developers are constantly working on making our products more secure.

This page will provide information about recent security vulnerabilities, what to do in the event of a security vulnerability affecting your system: [www.sick.com/psirt](http://www.sick.com/psirt).

#### 1.1.2 Reporting Security Vulnerabilities

All security issues should be reported to the SICK Product Security Incident Response Team (SICK PSIRT).

Details about the content and the process to follow are available here: [www.sick.com/psirt](http://www.sick.com/psirt).

**Note:** Please read our **Information Handling Policies** before sending us any details.

### 1.2 Further product information

Related documents:

- picoScan150 2D LiDAR sensor (8028323)

# 1 ABOUT THIS DOCUMENT

---

Operating instructions. This document provides important information on how to handle LiDAR from SICK AG and shows how to send telegrams via a terminal program using the SICK protocols to LiDAR from SICK AG.

- Data format description MSGPACK, Compact (8028132)

This document shows the structure and how to use the data streaming formats MSGPACK and Compact.

Please refer to the device product's operating instructions for information how to configure specific settings:

The page can be accessed via the SICK Product ID: [pld.sick.com/{P/N}/{S/N}](http://pld.sick.com/{P/N}/{S/N})

{P/N} corresponds to the part number of the product, see type label.

{S/N} corresponds to the serial number of the product, see type label (if indicated).

## 1.3 Legal notice

The application graphics and project planning examples contained in this manual, and their recommended settings, are not legally binding. They make no claim to be accurate or complete. They serve only as product demonstrations and do not represent customer specific solutions in any way.

The application graphics, the recommendations and project planning examples and their recommended settings are not a suitable replacement for necessary technical advice provided by a specialist. The specifications given in the product data sheets for the products described in this manual take precedence.

SICK cannot accept liability for any damage occurring outside the scope of the conditions described below. We retain the right to make changes to the application graphics and project planning examples, and their recommended settings, at any time without prior notice.

## 1.4 Liability

SICK will only accept liability for damage, for whatever legal reasons, in the following cases:

- for intent,
- gross negligence of the bodies or management employees,
- culpable injury to life, limb or health,
- faults which SICK maliciously failed to disclose,
- if SICK has offered a guarantee of a certain property of the supplied product,
- if SICK has offered a guarantee that the supplied product would have a certain property for a specific duration of time, and
- if it is found to be liable for personal injury or damage to private property under the German Product Liability Act.

If there is a breach of essential contractual obligations, SICK accepts liability in the case of gross negligence of non-management employees and in the case of slight negligence; however, in the latter case liability is limited to contractual damage that can be reasonably foreseen.

Essential contractual obligations are duties that protect the contractual legal positions of a party, which are intended to protect said party under the content and purpose of the contract. Furthermore, essential contractual obligations are duties that must be

performed in order for the contract to be properly fulfilled and which a contractual party expects and can expect to be met. Further claims to compensation are excluded.

### 2 General recommendations

#### 2.1 Intended use

The picoScan150 2D LiDAR sensor is a non-contact distance measuring sensor with one scan plane. It has been designed for indoor or outdoor and mobile or stationary use in stand-alone operation. Depending on the configuration and application software, the following usage scenarios can be solved:

- Detection of objects during continuous output of measurement data as required.
- Field monitoring of freely defined areas with signaling of object detection via digital outputs or telegrams.

It is suitable for applications which demand precise, non-contact optical measuring contours and dimensioning. Typical fields of application are, for example, stationary field protection, area monitoring, access control, mobile applications (navigation and anti-collision of mobile platforms) as well as profile detection. It can also be used, for example, to implement systems for collision protection, object protection or access monitoring.

The device is designed for use in industrial and logistics areas, and meets the requirements for industrial ruggedness, interfaces and data processing.

Only use the device in industrial environments (EN 61000-6-4).

Incorrect use, improper modification, or tampering with the product will invalidate any warranty offered by SICK AG. Furthermore, SICK AG shall not accept any responsibility or liability for any resulting damage and consequential damage.

#### 2.2 Environmental influences

In outdoor monitoring, fog, steam, dust, rain, or snow may physically affect the detection range. The extent to which the scanning range might be affected in this case can only be quantified in a specific verification test on site.

#### 2.3 Physical access restriction

The device should be operated in a protected area where only instructed and approved personnel have access.

#### 2.4 Limit exposure to public networks

It is not recommended to use picoScan150 in public networks. Using picoScan150 within an isolated network is a common and recommended measure to reduce exposure and risks.

#### 2.5 Elaborate an update strategy

The firmware of the device can be updated. It is recommended to use the latest version available. Start by searching on <https://supportportal.sick.com> or on [www.sick.com](http://www.sick.com) for the product and check “Downloads” for the latest “Firmware version”.



Checks for updates should be performed on a regular basis and applied as they are available. SICK recommends to test updates in your specific setting before rolling out an update on larger scale.

## 2.6 Configuration backup and restore

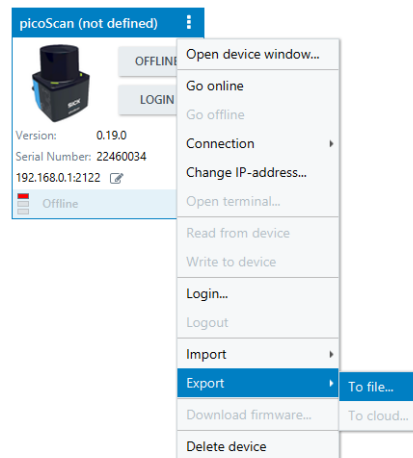
The functional scope of the device depends on the selected configuration. Certain functions are supported or not supported, depending on the configured variant.

It is recommended to have a backup of a known working configuration. If it comes to reinstallation or reconfiguration of the firmware to a secure state, a backup of the configuration file should be considered.

### 2.6.1 Backup (export)

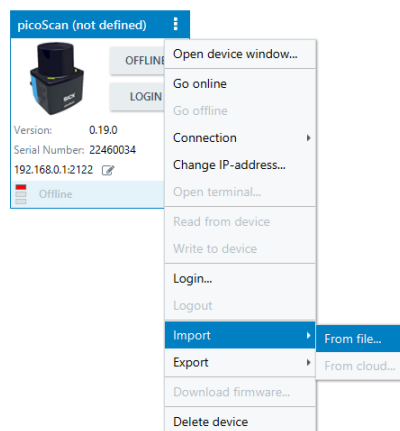
Start the configuration software SOPAS ET provided by SICK (available at [www.sick.com](http://www.sick.com))

Export the sensor configuration by using “Export to file” functionality. The configuration will be stored in a \*.sopas file.



### 2.6.2 Restore (import)

To import your configuration again, just use the “Import from file” functionality and select a \*.sopas file.



## 2 GENERAL RECOMMENDATIONS

### 2.7 Data integrity

A separate hash value is provided for all files belonging to the device (for example: \*.spk or \*.sdd).

Instructions for manually verifying the data are available at the following link:

<https://www.sick.com/verify-downloads>

The customer is free to choose how to calculate the hash value.

### 2.8 Brute-force

The device offers brute-force protection. After five consecutive unsuccessful login attempts, the device goes into a time lock of 30 seconds.

### 2.9 Periodic test

It is recommended to control the functionality of the security system on a regular basis. Please check the system that it is working as intended and document the result accordingly.

### 2.10 Device Identification

It is recommended to check that the correct type of the device and system-plug is connected to the system. The product ID is used as a unique identifier. The product ID consists of the product number and serial number. You will find the label on the device and system-plug.



The product ID can also be read out via the UI. Example:



The screenshot also shows the version of the device's currently used firmware. The format of the firmware version follows Semantic Versioning. Example: Firmware version 1.23.0

This document is valid for all picoScan150 variants.

Additionally, it can be checked by using telegrams, see Telegram listing in the operating instructions (8028323)

Example: Read device order number: **sRN OrdNum**

## 2.11 Use Device-Not-Ready status

The device has a Device-Not-Ready status, which signals that the device is not operating correctly. This status can be observed by communication or by digital output. Changes of the Device-Not-Ready state may be used as a manipulation warning, i.e. Device-Not-Ready changes while the device parameter are changed.

Refer operating instructions for more details.

## 3 PROTECTION LEVELS

### 3 Protection Levels

This device guide uses different protection levels depending on system size and needs. Each level assumes that the previous level's recommendations are followed:

Protection level	Use for	Procedures
No protection	Demo purposes or test scenarios	<ul style="list-style-type: none"><li>• Set factory default</li></ul>
Basic protection	Recommended minimum level. Reduces most common risks. Assumes low criminal energy.	<ul style="list-style-type: none"><li>• Check for latest firmware / release notes</li><li>• Change all passwords</li><li>• Configure network settings</li><li>• Disconnect unused interfaces</li><li>• Close unused ports / services</li></ul>
Advanced protection	Recommended settings for exposed or critical systems. Assumes advanced criminal energy.	<ul style="list-style-type: none"><li>• Limit network access (IP-range)</li></ul>

#### 3.1 No protection

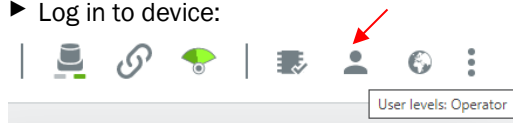
In no protection, there are no access restrictions. The passwords are on default and the interfaces are active. It is not recommended to use these settings for daily operations but only for Demo or Test installations.

This mode should be used in daily operations only if the device has restricted physical access and is not connected to a network or other protection i.e. firewall is implemented.

##### 3.1.1 Set factory default

Start with setting defaults to ensure proper device factory defaults.

► Log in to device:



### Logging into the device

Select a user level, enter the password and optionally activate expert mode.

User levels

Password

[Password forgotten?](#)

**Log in**

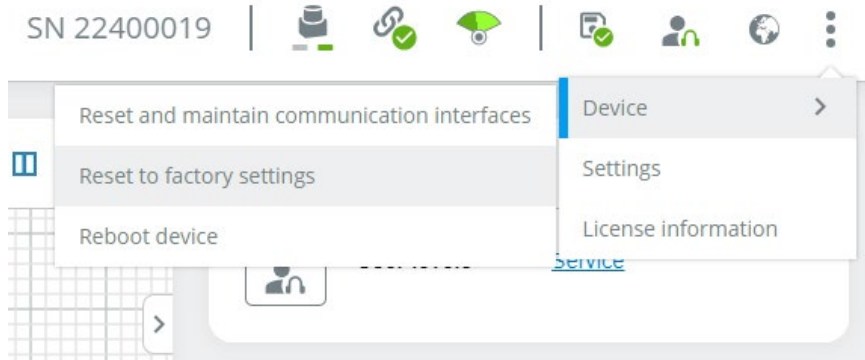
- ▶ User level: Service  
Default password: servicelevel
- ▶ Check correct user level:



Log in

User levels [Service](#)

- ▶ Set factory defaults in device.



Factory settings

The device will be reset to factory settings. The IP address is reset to 192.168.0.1. You can only connect to the device via this IP address after permanently saving it and restarting the device. Do you want to reset the device to factory settings?

Cancel Yes

The device will set factory defaults including the default passwords and reboot.

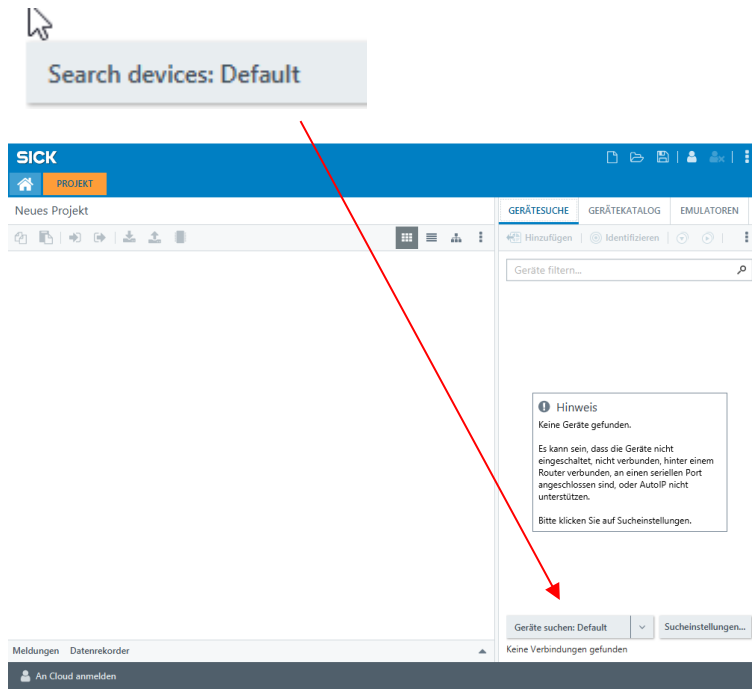
The device will reboot with the standard IP address 192.168.0.1

In case a specific IP address was used before:

- the device IP address must be set to default in web browser or

### 3 PROTECTION LEVELS

- the device needs to be searched and reconnected in the SOPAS main window



### 3.2 Basic protection

The basic protection level is the minimum recommended level for daily operation in uncritical environment.

#### 3.2.1 Check for latest firmware / release notes

Occasionally critical vulnerabilities are discovered during lifecycle of devices and a firmware update is necessary. Updating firmware is an important aspect of cybersecurity.

Before setting up the device, make sure to use the latest firmware. The release notes of the firmware contains information of included security patches.

To check for the latest firmware and release notes, start by searching on <https://supportportal.sick.com> for the product and check “Downloads” for the latest “Firmware Version” and “Release Notes”.

#### 3.2.2 Change passwords

Change the default passwords in all user levels (Maintenance personnel, Authorized client and Service) to unique ones. Use strong passwords and keep it secret. This is the main access protection of the device.

User level	Default password
Operator	No password required
Maintenance personnel	main
Authorized client	client
Service	servicelevel

The assignment of a new password is secured by the old password. Therefore, it is recommended to pay special attention to the confidentiality of the connection when

assigning the password for the first time, for example, by using a point-to-point connection to the device.

**Password strength recommendation:**

Passwords should include the following characters:

- capital letters
- lowercase letters
- special character
- numbers

When logging in for the first time, you will be prompted to change your password. There are following options

- „New password“ (different from default recommended)
- „Keep default password“
- „Skip“ (dialog appears again at the next login)

Create password ×

You are logging in for the first time, change your password to a unique one.

👁

👁

Skip
Change

---

Keep default password

**3.2.3 Password reset**

The password of user level Service only, can be reset to default using the “Password reset” process. Following steps are required:

- ▶ Click on „Password forgotten“

### 3 PROTECTION LEVELS

---

#### Logging into the device

Select a user level, enter the password and optionally activate expert mode.

User levels

Password

[Password forgotten?](#)

**Log in**

- ▶ Send this e-mail to the responsible SICK sales company or service partner, see [www.sick.com/worldwide](http://www.sick.com/worldwide)

Resetting the password ×

Send the following data to your SICK service technician. After successful processing, you will receive a code that you can enter in the next step.

Device key

Serial number

Part number

[Generate e-mail with data](#)

**Next**

- ▶ Paste the “Code” from the received e-mail and click button **Reset**.



Resetting the password ×

[← Back](#)

Enter the code here that you received from SICK. After successful entry, the current password is reset to the default password.

Code

[Cancel](#)

[Reset](#)

✓ The password has been reset to the default password ×

The Cancel button aborts the password reset process and a new reset code must be requested from manufacturer.

Resetting the password ×

Are you sure to cancel this process? If you cancel the process, the requested code is no longer valid and you must restart the process.

[No](#)

[Yes](#)

### 3.2.4 Configure Network Settings

Device network defaults are:

- IP address: 192.168.0.1
- Subnet mask: 255.255.255.0
- Default gateway: 0.0.0.0
- TCP port: 2111, 2112, 2122

### 3.2.5 Disconnect unused interfaces

If the communication interface isn't used for your application, please disconnect the communication cable to harden your system.

### 3 PROTECTION LEVELS

---

Example:

The application uses only the digital I/O`s and the communication interface is only used for parameterization.

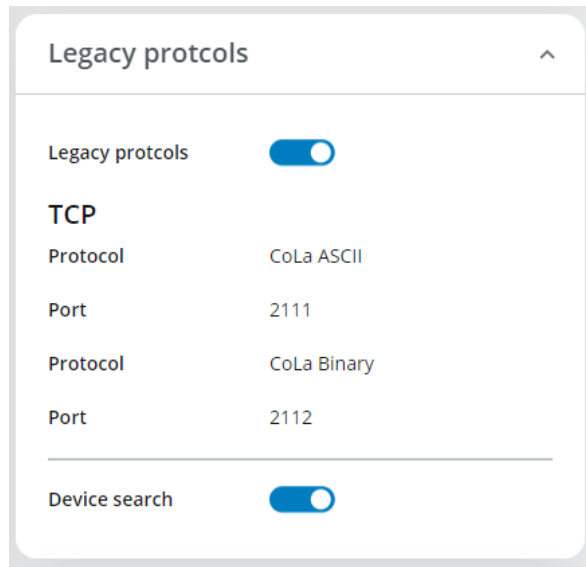
#### 3.2.6 Close unused ports / services

Disabling unused interfaces and protocols is an important step to reduce the attack surface. It is recommended to disable all protocols not used for operation.

##### 3.2.6.1 Legacy protocols

Connection options. Login as Service.

*Configuration > Connection options > Legacy protocol*



#### **TCP – CoLa1**

CoLa1 (CoLa ASCII / Binary) is active by default.

Intended use:

Configuration and status request of the sensor via telegrams. See chapter telegram listing in the operating instructions (8028323)

Please note: CoLa1 (CoLa ASCII / Binary) is not recommended, because this protocol is deprecated.

#### **Device search**

Device search is active by default. Device search uses port 30718/udp

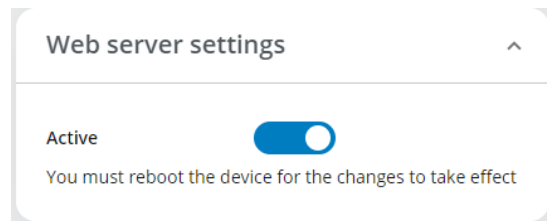
Intended use:

Search any SICK device in your connected network.

##### 3.2.6.2 Web server settings

Connection options. Login as Service.

Configuration > Connection options > Web server settings



**Webserver**

Webserver (Port 80) is active by default.

Intended use:

Interaction (visualization, parameterization) with the sensor by using the web browser interface.

If the port is disabled, the sensor will be only reachable by using SOPAS ET.

**3.2.6.3 CoLa2**

Connection options. No login necessary

Configuration > Connection options > CoLa 2



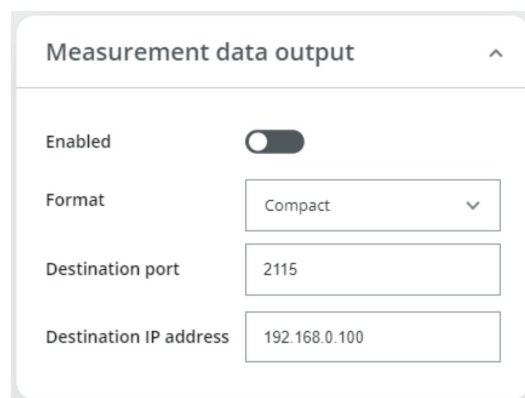
TCP – CoLa2

CoLa2 connection via TCP port 2122 is considered a vital part of the intended use, which is why not being able to switch off.

**3.2.6.4 Measurement data output**

Data output. Login as Authorized client.

Application > Data output > Measurement data output



### 3 PROTECTION LEVELS

---

#### UDP

Measurement data output (UDP Streaming) is inactive by default.

Intended use:

Streaming of the measurement data

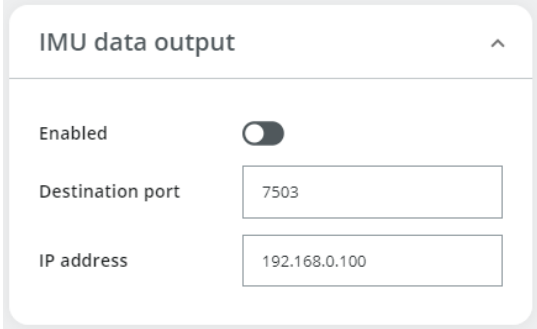
Activating the measurement data output opens a new, device-side UDP port each time.

If the measurement data output is deactivated again, this also closes the device-side UDP port.

#### 3.2.6.5 IMU data output

Data output. Login as Authorized client.

*Application > Data output > IMU data output*



The screenshot shows a configuration window titled "IMU data output" with a close button (caret) in the top right corner. It contains three settings:

- Enabled:** A toggle switch that is currently turned off.
- Destination port:** A text input field containing the value "7503".
- IP address:** A text input field containing the value "192.168.0.100".

#### UDP

IMU data output (UDP Streaming) is inactive by default.

Intended use:

Streaming of the IMU data

Activating the IMU data output opens a new, device-side UDP port each time.

If the IMU data output is deactivated again, this also closes the device-side UDP port.

#### 3.2.6.6 Digital IOs

Inputs and outputs. Login as Authorized client.

*Configuration > Inputs and outputs*

The image displays three identical configuration panels for ports 'InOut1', 'InOut2', and 'InOut3'. Each panel includes a 'Port name' field, radio buttons for 'Input' and 'Output' (with 'Output' selected), an 'Add source' button, a 'Restart' dropdown set to 'Immediate', a 'Status (log.)' indicator, a 'Logic' dropdown set to 'Active High', an 'Output mode' dropdown set to 'PNP', and a 'Status (phys.)' indicator. To the right of each panel is a circular diagram representing a physical port with pins, numbered 4, 2, and 5 respectively.

Intended use:

Digital signal for device specific applications signals e.g. DeviceNotReady or different Evaluations

### 3.2.6.7 Date and system time

Basic settings. Login as Authorized client.

Configuration > Basic settings > Date and system time

The screenshot shows the 'Date and system time' configuration window. It contains the following settings:

- Synchronization:** A dropdown menu set to 'NTP'.
- Time server IP address:** A text input field containing '192.168.0.11'.
- Update time:** A control with minus and plus buttons, a central input field with '600', and a unit indicator 's'.
- Time zone:** A dropdown menu set to 'AMSTERDAM\_BER...'.

### 3 PROTECTION LEVELS

---

#### UDP

NTP (UDP request) is inactive by default.

Intended use:

Synchronized date and system time

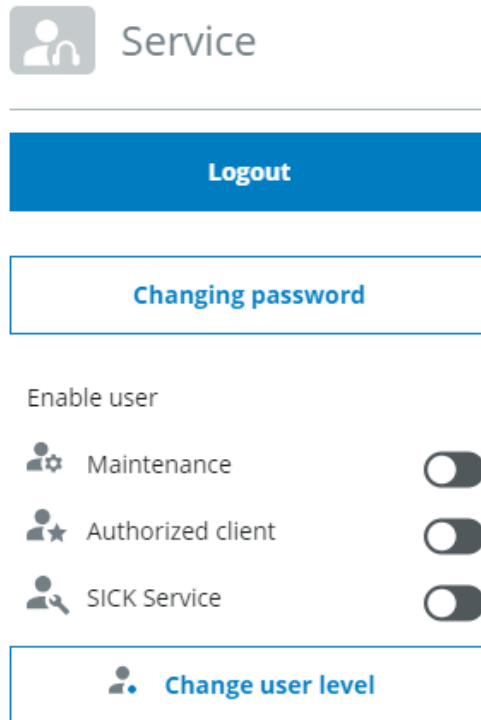
Activating the NTP opens a new, device-side UDP port each update time.

If the NTP is deactivated again, no more device-side UDP port is opened each update time.

#### 3.2.6.8 User levels

All user levels are inactive by default, except user level Service. User level Service cannot be deactivated and is therefore always active.

To activate other user levels, you must log in with user level Service first.



#### 3.2.6.9 SICK Service

User level SICK Service is inactive by default. Login as Service.

The user level SICK service is for maintenance purposes only and should only be activated if requested by the manufacturer.

### 3.3 Advanced protection

The advanced settings are additionally to the basic settings.

#### 3.3.1 Limit network access (IP-range)

Change default IP address to non-default values.

Limit the subnetmask to your specific subnet: as small as possible, as big as necessary.

Subnetting divides larger networks into smaller parts, which is more efficient and saves a large number of addresses. The smaller networks therefore generate less broadcast and thus less broadcast traffic. Subnetting also makes troubleshooting easier by isolating network problems back to their source.

Connection options. Login as Service

*Configuration > Connection options > Ethernet*

The screenshot shows the 'Ethernet' configuration window. It contains the following fields and values:

- Addressing mode:** Static (dropdown menu)
- IP address:** 192.168.0.1
- Subnet mask:** 255.255.255.0
- Default gateway:** 0.0.0.0
- MAC address:** 00:06:77:00:00:00
- Calculated speed:** 100 Mbit/s full duplex (dropdown menu)

An 'Apply' button is located below the Default gateway field.

### 4 Application related recommendations

#### 4.1 Primary sensor data

##### 4.1.1 Measurement data output

The device provides the distance measurement data as raw data (MSGPACK format and Compact format) for customer applications. To increase the security and integrity of the measurement data we propose the following security measures.

**Remark:**

For requesting data from device, please refer for additionally information: Telegram listing (8028323) and Data format description MSGPACK, Compact (8028132).

##### 4.1.1.1 MSGPACK format

The data packets transmitted in MSGPACK format are enclosed in a framing consisting of a header before the actual user data and a checksum after the user data.

The header of the MSGPACK format provides the following security and integrity related information.

**Telegram Counter**

Counts all telegrams sent with measurement data in MSGPACK format since the unit was switched on. The counter starts with 1.

The counter can be used to check if any data got lost in the data stream.

**Time Stamp Transmit**

Sensor system time in  $\mu\text{s}$  since 1.1.1970 00:00 in UTC. If a time server is used, the sensor can be synchronized to that.

The timer can be used to check if there are time delays in the data stream.

**Segment Counter**

The device is able to stream data by segments to increase the reaction time of following data analysis. One frame (e.g.  $276^\circ$ ) is split into 10 segments by  $30^\circ$  or 5 segments by  $60^\circ$ .

**Frame Number**

Count the number of frames (e.g.  $276^\circ$ ) since the start of the device.

The counter can be used to check if any data got lost in the data stream.

**Sender ID**

Serial number of the device.

It can be used to identify on the receiver from which sensor the data was sent.

The MSGPACK format provides a checksum after the user data.

**CRC32 checksum**

The CRC32 checksum, which follows the user data, is calculated over the entire data packet, i.e. over the header and the serialized scan segment.



#### 4.1.1.2 Compact format

The data packets transmitted in Compact format are enclosed in a framing consisting of a header before the actual user data and a checksum after the user data.

The header of the compact format provides the following security and integrity related information.

##### Command ID

Defines the type of the transmitted telegram. For data serialization **the Command ID is 1.**

The Command ID can be used to differentiate between sensor data types (e.g. measurement data, IMU data).

##### Telegram Counter

Counts all telegrams which have been created since power up. The counter starts with 1.

The counter can be used to check if any data got lost in the data stream.

##### Time Stamp Transmit

Sensor system time since 1.1.1970 00:00 in UTC [ $\mu$ s].

The timer can be used to check if there are time delays in the data stream.

##### Telegram Version

Version of the serialization telegram. **Allowed versions are 3 and 4.**

Telegram version can be used to trace any telegram changes.

The compact format provides a checksum after the user data.

##### CRC32 checksum

The CRC32 checksum, which follows the user data, is calculated over the entire data packet, i.e. over the header and the serialized scan segment.

## 4.2 Secondary sensor data

### 4.2.1 IMU data output

The device provides the IMU data output for customer applications. To increase the security and integrity of the measurement data we propose the following security measures.

### 4.2.2 Command ID

Defines the type of the transmitted telegram. For IMU data serialization **the Command ID is 2.**

The Command ID can be used to differentiate between sensor data types (e.g. measurement data, IMU data).

### 4.2.3 Telegram Version

Version of the serialization telegram. For the telegram structure described in this requirement the **telegramVersion is 1.**

Telegram version can be used to trace any telegram changes.

## 4 APPLICATION RELATED RECOMMENDATIONS

### 4.2.4 IMU Sensor Timestamp

Sensor system time since 1.1.1970 00:00 in UTC.

The timer can be used to check if there are time delays in the data stream.

### 4.2.5 CRC32 checksum

CRC32 of all words except the checksum.

## 4.3 Device state

Monitoring of the device state to detect changes in the parameterization.

The general device state of the device is transmitted via the following telegram:

- sRN SCdevicestate

The device status can be read out via the following telegram

- sRN DeviceStatus

## 4.4 Recommended Security measures

### 4.4.1 Last Modified

Secure the last modified information when the device parameter was changed and stored.

*Diagnosis > Overview > Operating information*

Operating information	
Power-on counter	690
Operating hours	
Since switching on	0 h
Total	742.9 h
Last parameterization	20.12.2022 12:03
Temperature	48.4 °C

### 4.4.2 Messages

The device provides a diagnostic overview. It is recommended to control this functionality on a regular basis. If the sensor is not working as intended, the troubleshooting section provides information on how to fix the problem and how to proceed, if the operator is not able to fix the problem on his own.

*Diagnosis > Overview > Messages*

Date	Status	Troubleshooting process
No entries available		

### 4.4.3 Diagnostic file


The device provides a diagnostic file for deep dive analysis. Only SICK internal readable. Log in as Service.

*Diagnostics > Overview > Diagnostic file*


Diagnostic file was created on 01.01.1970 at 02:00.

 Download

Create a diagnostic file for error analysis.

 **Caution**

Creating a diagnostic file overwrites the current diagnostic file, which can then no longer be downloaded.

 Create file

### 4.4.4 Changing Parameter

Prevent changing parameter by unauthorized operators. By changing parameter, the application result can be changed. Limit access to the device parameter to the minimum amount of people (need-to-know principle).

**Australia**

Phone +61 (3) 9457 0600  
1800 33 48 02 – tollfree  
E-Mail sales@sick.com.au

**Austria**

Phone +43 (0) 2236 62288-0  
E-Mail office@sick.at

**Belgium/Luxembourg**

Phone +32 (0) 2 466 55 66  
E-Mail info@sick.be

**Brazil**

Phone +55 11 3215-4900  
E-Mail comercial@sick.com.br

**Canada**

Phone +1 905.771.1444  
E-Mail cs.canada@sick.com

**Czech Republic**

Phone +420 234 719 500  
E-Mail sick@sick.cz

**Chile**

Phone +56 (2) 2274 7430  
E-Mail chile@sick.com

**China**

Phone +86 20 2882 3600  
E-Mail info.china@sick.net.cn

**Denmark**

Phone +45 45 82 64 00  
E-Mail sick@sick.dk

**Finland**

Phone +358-9-25 15 800  
E-Mail sick@sick.fi

**France**

Phone +33 1 64 62 35 00  
E-Mail info@sick.fr

**Germany**

Phone +49 (0) 2 11 53 010  
E-Mail info@sick.de

**Greece**

Phone +30 210 6825100  
E-Mail office@sick.com.gr

**Hong Kong**

Phone +852 2153 6300  
E-Mail ghk@sick.com.hk

**Hungary**

Phone +36 1 371 2680  
E-Mail ertesites@sick.hu

**India**

Phone +91-22-6119 8900  
E-Mail info@sick-india.com

**Israel**

Phone +972 97110 11  
E-Mail info@sick-sensors.com

**Italy**

Phone +39 02 27 43 41  
E-Mail info@sick.it

**Japan**

Phone +81 3 5309 2112  
E-Mail support@sick.jp

**Malaysia**

Phone +603-8080 7425  
E-Mail enquiry.my@sick.com

**Mexico**

Phone +52 (472) 748 9451  
E-Mail mexico@sick.com

**Netherlands**

Phone +31 (0) 30 229 25 44  
E-Mail info@sick.nl

**New Zealand**

Phone +64 9 415 0459  
0800 222 278 – tollfree  
E-Mail sales@sick.co.nz

**Norway**

Phone +47 67 81 50 00  
E-Mail sick@sick.no

**Poland**

Phone +48 22 539 41 00  
E-Mail info@sick.pl

**Romania**

Phone +40 356-17 11 20  
E-Mail office@sick.ro

**Russia**

Phone +7 495 283 09 90  
E-Mail info@sick.ru

**Singapore**

Phone +65 6744 3732  
E-Mail sales.gsg@sick.com

**Slovakia**

Phone +421 482 901 201  
E-Mail mail@sick-sk.sk

**Slovenia**

Phone +386 591 78849  
E-Mail office@sick.si

**South Africa**

Phone +27 10 060 0550  
E-Mail info@sickautomation.co.za

**South Korea**

Phone +82 2 786 6321/4  
E-Mail infokorea@sick.com

**Spain**

Phone +34 93 480 31 00  
E-Mail info@sick.es

**Sweden**

Phone +46 10 110 10 00  
E-Mail info@sick.se

**Switzerland**

Phone +41 41 619 29 39  
E-Mail contact@sick.ch

**Taiwan**

Phone +886-2-2375-6288  
E-Mail sales@sick.com.tw

**Thailand**

Phone +66 2 645 0009  
E-Mail marcom.th@sick.com

**Turkey**

Phone +90 (216) 528 50 00  
E-Mail info@sick.com.tr

**United Arab Emirates**

Phone +971 (0) 4 88 65 878  
E-Mail contact@sick.ae

**United Kingdom**

Phone +44 (0)17278 31121  
E-Mail info@sick.co.uk

**USA**

Phone +1 800.325.7425  
E-Mail info@sick.com

**Vietnam**

Phone +65 6744 3732  
E-Mail sales.gsg@sick.com

**South Korea**

Phone +82 2 786 6321  
E-Mail info@sickkorea.net

**Spain**

Phone +34 93 480 31 00  
E-Mail info@sick.es

**Sweden**

Phone +46 10 110 10 00  
E-Mail info@sick.se

**Switzerland**

Phone +41 41 619 29 39  
E-Mail contact@sick.ch

**Taiwan**

Phone +886 2 2375-6288  
E-Mail sales@sick.com.tw

**Thailand**

Phone +66 2645 0009  
E-Mail Ronnie.Lim@sick.com

**Turkey**

Phone +90 216 528 50 00  
E-Mail info@sick.com.tr

**United Arab Emirates**

Phone +971 4 88 65 878  
E-Mail info@sick.ae

**United Kingdom**

Phone +44 1727 831121  
E-Mail info@sick.co.uk

**USA**

Phone +1 800 325 7425  
E-Mail info@sick.com

**Vietnam**

Phone +84 945452999  
E-Mail Ngo.Duy.Linh@sick.com

Detailed addresses and further locations at  
[www.sick.com](http://www.sick.com)