TECHNICAL INFORMATION

LMS5xx Hardening Guide

SICK
Sensor Intelligence.

Described Product

LMS5xx

Manufacturer

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

Legal information

Original document

This document is an original document of SICK AG.

Content

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 LMS5xx:

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

This document provides technical advice for anyone involved in deploying LMS5xx.

Version of this document: V2.0.0 (adapted to Hardware Revision II with firmware V2.x)

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**.

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**.

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**.

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

1.2 Further product information

Please refer to the LMS5xx Operating instructions for information how to configure specific settings. This and other related documents and information can be found on the product page.

The page can be accessed via the SICK Product ID: pid.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.

2 General recommendations

2.1 Intended use

The LMS5xx is a non-contact optical distance measurement sensor in standalone or network operation based on a 2D-LiDAR sensor. It is suitable for applications which demand precise, non-contact optical measuring contours and dimensioning. It can also be used to implement systems for collision protection, object protection or access monitoring, for example.

The device may only be put into operation by authorized staff and only in industrial environments.

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

It is not recommended to use LMS5xx in public networks. Using LMS5xx within an isolated network is a common and recommended measure to reduce exposure and risks.

2.2 Elaborate an update strategy

The firmware of the device can be updated. It is recommended to use the latest version available.

The latest version of the firmware can be found on the product page in the section “Downloads”.

The page can be accessed via the SICK Product ID: pid.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).

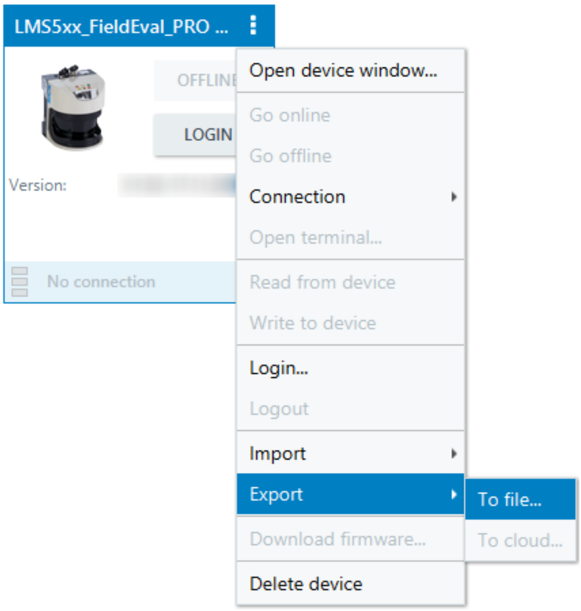
Checks for updates should be performed on a regular basis and applied as they are available. SICK recommends to test updates in your specific setting before rolling out an update on larger scale.

2.3 Configuration backup and restore

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.

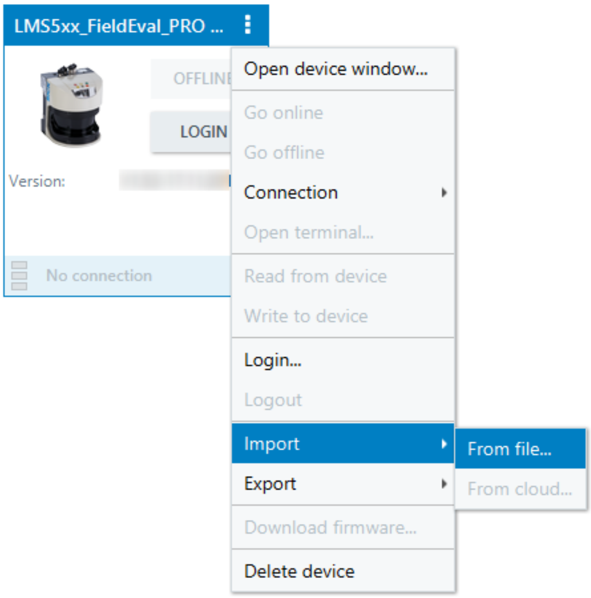
2.3.1 Backup (export)

In software SOPAS ET, export the sensor configuration by using “Export to file” functionality. The configuration will be stored in a *.sopas file.



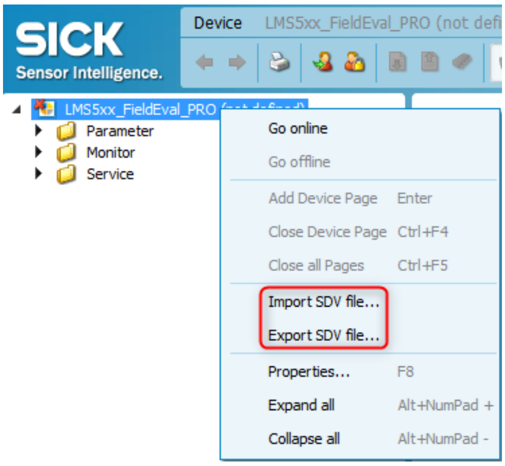
2.3.2 Restore (import)

It is very easy to import your configuration again. In SOPAs ET, use the “Import from file” functionality and select a *.sopas file.



Remark:

The *.sdv file format is deprecated.



2.4 Periodic walk test (available in LMS531 only)

It is recommended to control the functionality of the security system on a regular basis. To do that the object that should be detected should be moved within the borders of the detection area. The constant detection of the object shall be verified by monitoring the output of the device or the alarm status that is triggered by the device.

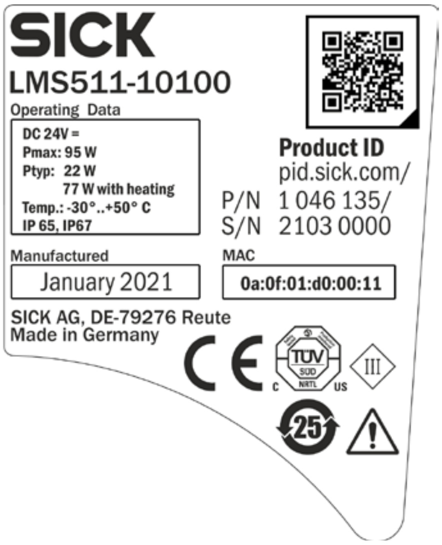
“walk test”: The Front panel is active and field infringement will be displayed on the “Q1” LED and alarm output switches. The 2nd input has a higher priority than 1st input. So if “walk test” is active the “Armed/Disarmed” mode is disregarded.

Additionally the input “functional test” can be switched on. The display of the device will be switched on. An object detection will be indicated by the yellow LED on the display.

2.5 Device Identification

It is recommended to check that the correct type of LMS5xx is connected to the system. This can be done with the information on the type label.

Example LMS511:



Additionally, it can be checked by using telegrams.

Example:
Read device order number: `sRN DIornr`

Regarding telegrams, see also publication “Telegram listing”, which can be found on the product page.

The page can be accessed via the SICK Product ID: pid.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).

2.6 Use Device-Not-Ready status

The LMS5xx has a Device-Not-Ready status, which signals that the device is not operating correctly. This status can be observed by telegram 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 parameters are changed.

Remark:

The LMS531 uses the name “Device-Ready”.

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	Used for	Procedures
No protection	Demo purposes or test scenarios	• Set factory default
Basic protection	Recommended minimum level. Reduces most common risks. Assumes low criminal energy.	• Check for latest firmware/ release notes • Change all passwords • Configure network settings • Disconnect unused interfaces
Advanced protection	Recommended settings for exposed or critical systems. Assumes advanced criminal energy.	• Switch off USB port and Display • Limit network access (IP-range)

3.1 No Protection

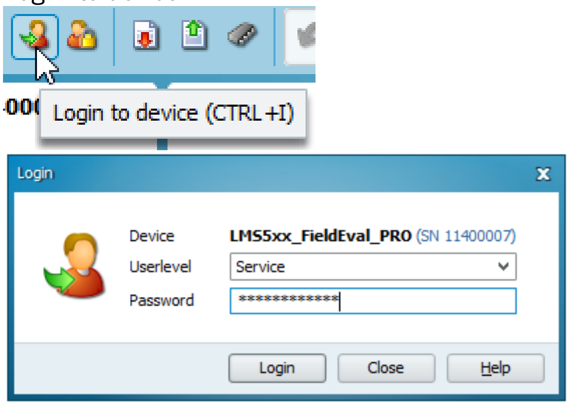
In level "no protection", there are no access restrictions. The passwords are on default and the interfaces are active. It is not recommended to use these settings for daily operations but only for Demo or Test installations.

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.

1. Log in to device:



Login to device (CTRL+I)

Login

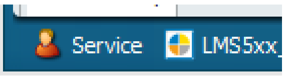
Device LMS5xx_FieldEval_PRO (SN 11400007)

Userlevel Service

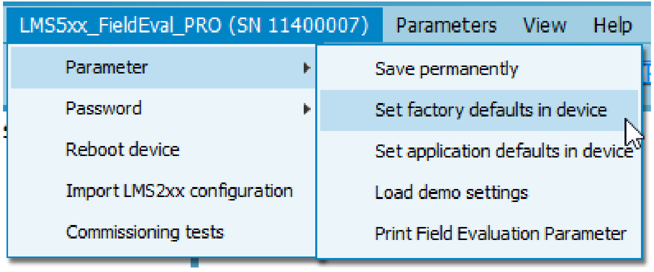
Password *************

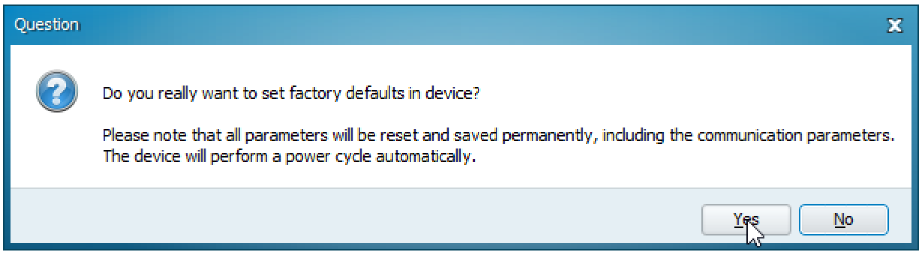
User level	Default password
Maintenance (Authorized Operator)	`main`
Authorized Client (Integrator)	`client`
Service	`servicelevel`

2. Check correct userlevel at left bottom corner of device window.



3. A) LMS531, LMS511 and LMS500:
“Set factory defaults in device” and confirm with “Yes”.


LMS5xx_FieldEval_PRO (SN 11400007)
Parameters
View
Help
Parameter
Password
Reboot device
Import LMS2xx configuration
Commissioning tests
Save permanently
Set factory defaults in device
Set application defaults in device
Load demo settings
Print Field Evaluation Parameter

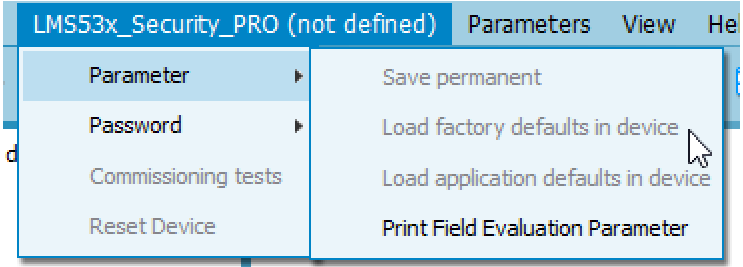


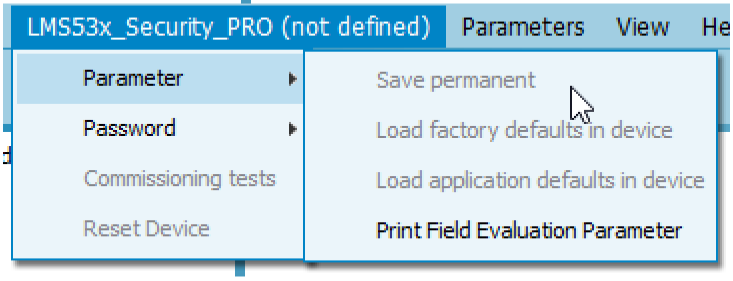
Do you really want to set factory defaults in device?

Please note that all parameters will be reset and saved permanently, including the communication parameters.
The device will perform a power cycle automatically.

The device will set factory defaults and reboot.

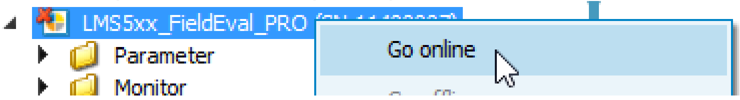
B) LMS531:
“Load factory defaults in device” and “Save permanent”.


LMS53x_Security_PRO (not defined)
Parameters
View
He
Parameter
Password
Commissioning tests
Reset Device
Save permanent
Load factory defaults in device
Load application defaults in device
Print Field Evaluation Parameter


LMS53x_Security_PRO (not defined)
Parameters
View
He
Parameter
Password
Commissioning tests
Reset Device
Save permanent
Load factory defaults in device
Load application defaults in device
Print Field Evaluation Parameter

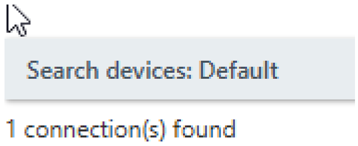
Reboot the LMS531 by powering it off and on again.

4. When the green LED is on again, right-click on the device name and reconnect:



The device will reboot with the standard IP address `192.168.0.1`

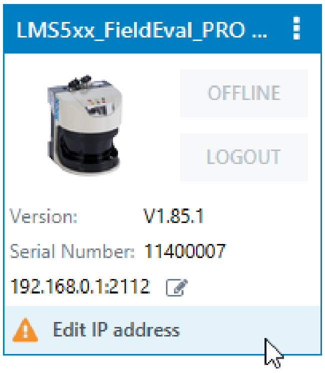
- ▶ In case a specific IP address was used before, the device needs to be searched and reconnected in the SOPAS main window:



Search devices: Default

1 connection(s) found

  - Drag + drop the device to the left side of the window and reconnect.
  - Change the IP address to the specific requirements.



LMS5xx_FieldEval_PRO ...

Version: V1.85.1

Serial Number: 11400007

192.168.0.1:2112

⚠ Edit IP address

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.

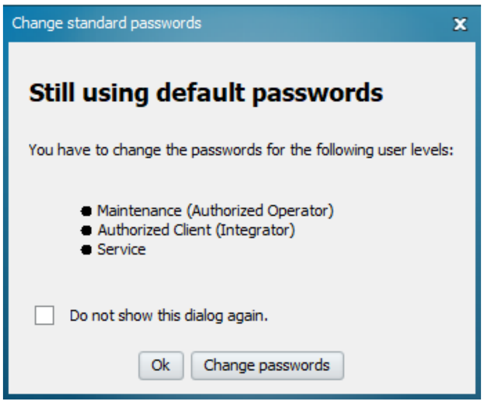
The latest firmware and release notes can be found on the product page.

The page can be accessed via the SICK Product ID: pid.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).

3.2.2 Change passwords



Change standard passwords

Still using default passwords

You have to change the passwords for the following user levels:

- Maintenance (Authorized Operator)
- Authorized Client (Integrator)
- Service

□ Do not show this dialog again.

Change the default passwords in all user levels (Maintenance, 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 (Authorized Operator)	`main`
Authorized Client (Integrator)	`client`
Service	`servicelevel`

Recommendation:

Passwords should include the following characters:

- capital letters
- lowercase letters
- special character
- numbers

3.2.3 Configure Network Settings

LMS5xx network defaults are:

- IP address: 192.168.0.1
- Subnet mask: 255.255.255.0
- TCP port: 2111, 2112

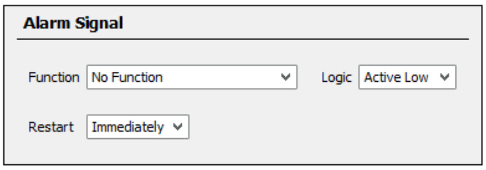
3.2.4 Disconnect unused interfaces

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.

LMS531 PRO digital outputs settings

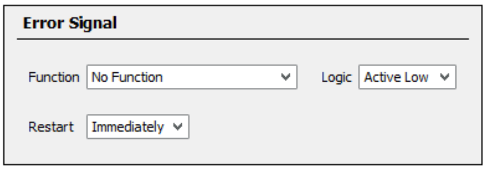
Login as Authorized Client (Integrator).

- ▶ Parameter > Network / Interfaces / IOs > Digital Outputs



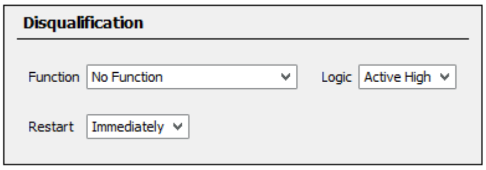
Alarm Signal

Function: No Function
Logic: Active Low
Restart: Immediately



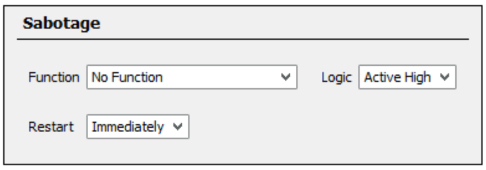
Error Signal

Function: No Function
Logic: Active Low
Restart: Immediately



Disqualification

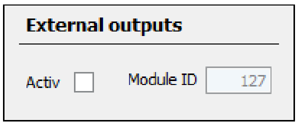
Function: No Function
Logic: Active High
Restart: Immediately



Sabotage

Function: No Function
Logic: Active High
Restart: Immediately

- ▶ Parameter > Network / Interfaces / IOs > External digital outputs



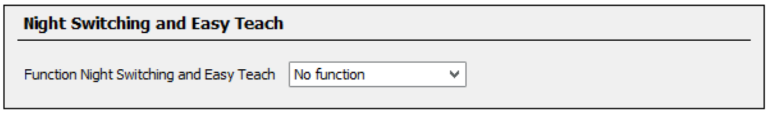
External outputs

Activ ☐
Module ID: 127

LMS531 PRO switching inputs settings

Login as Authorized Client (Integrator).

- ▶ Parameter > Network / Interfaces / IOs > Digital Inputs



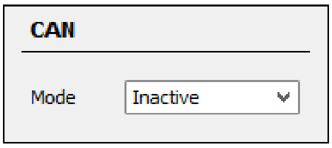
Night Switching and Easy Teach

Function Night Switching and Easy Teach: No function

LMS531 PRO interfaces

Login as Authorized Client (Integrator).

- ▶ Parameter > Network / Interfaces / IOs > CAN



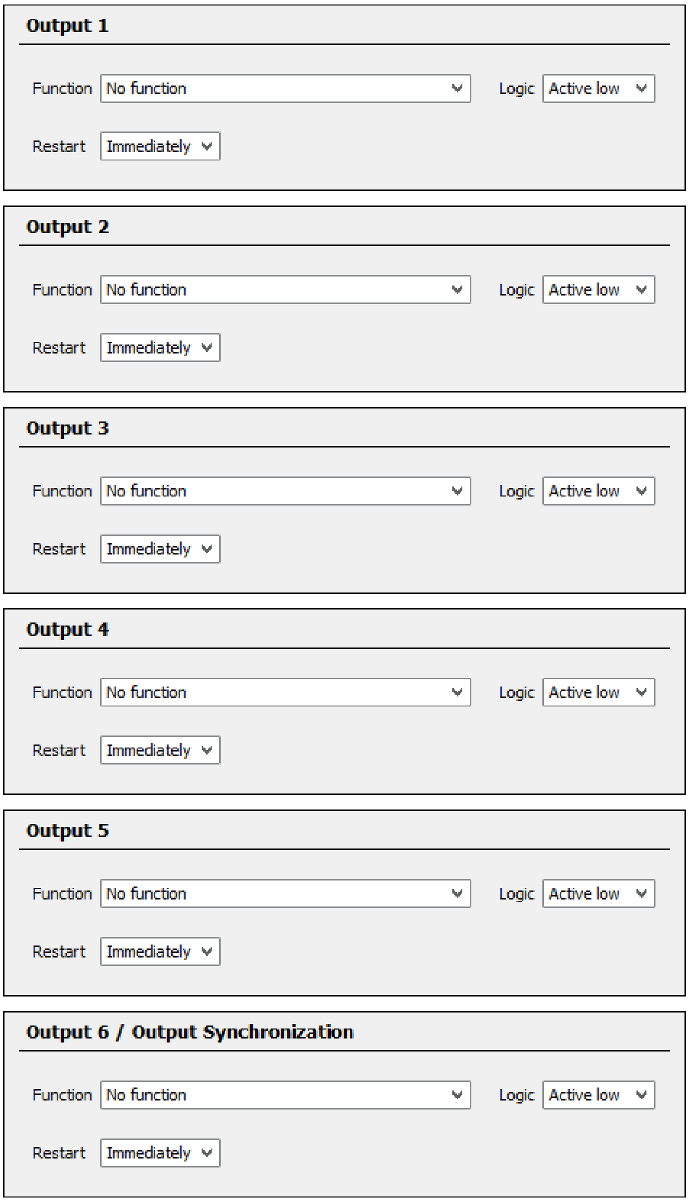
CAN

Mode: Inactive

LMS511 and LMS500 PRO digital outputs settings

Login as Service.

- Parameter > Network / Interfaces / IOs > Digital Outputs



Output 1

Function: No function
Logic: Active low
Restart: Immediately

Output 2

Function: No function
Logic: Active low
Restart: Immediately

Output 3

Function: No function
Logic: Active low
Restart: Immediately

Output 4

Function: No function
Logic: Active low
Restart: Immediately

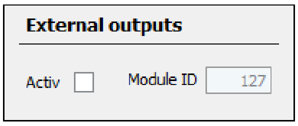
Output 5

Function: No function
Logic: Active low
Restart: Immediately

Output 6 / Output Synchronization

Function: No function
Logic: Active low
Restart: Immediately

- Parameter > Network / Interfaces / IOs > External digital outputs



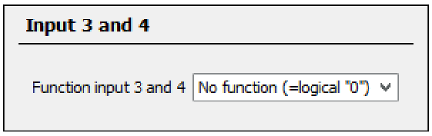
External outputs

Activ ☐ Module ID 127

LMS511 and LMS500 PRO switching inputs settings

Login as Service.

▶ Parameter > Network / Interfaces / IOs > Digital Inputs 3 +4 / Encoder (HTL) / Sync



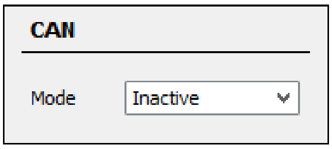
Input 3 and 4

Function input 3 and 4 No function (=logical "0")

LMS511 and LMS500 PRO interfaces

Login as Service.

▶ Parameter > Network / Interfaces / IOs > CAN



CAN

Mode Inactive

3.3 Advanced Protection

The advanced settings are additionally to the basic settings.

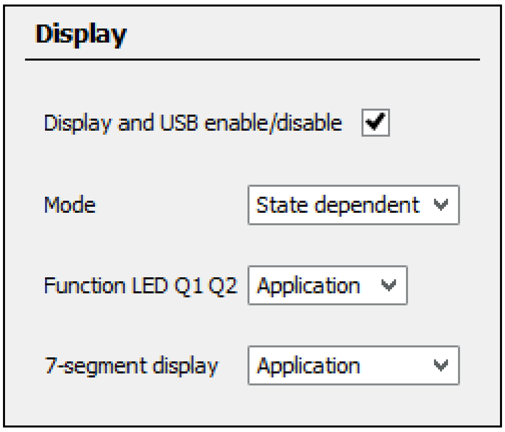
3.3.1 Switch off USB port and display

The display of the device shows the device status and the application status. The status gives information about the device, its function and its parametrization. Disable the display to avoid spying on the noticeable behavior of the device.

Exclusively with the LMS531 the USB port is also switched off in case the display is switched off.

LMS531

▶ Parameter > Network / Interfaces / IOs > Display



Display

Display and USB enable/disable ☑

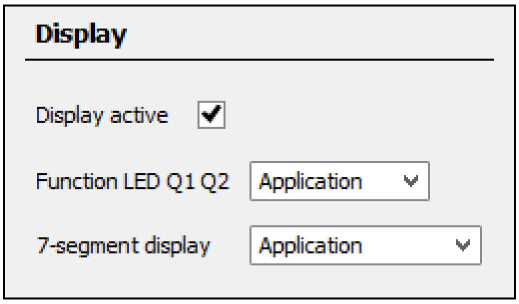
Mode State dependent

Function LED Q1 Q2 Application

7-segment display Application

LMS511 and LMS500

▶ Parameter > Network / Interfaces / IOs > Display



Display

Display active ☑

Function LED Q1 Q2: Application

7-segment display: Application

3.3.2 Limit network access (IP-range)

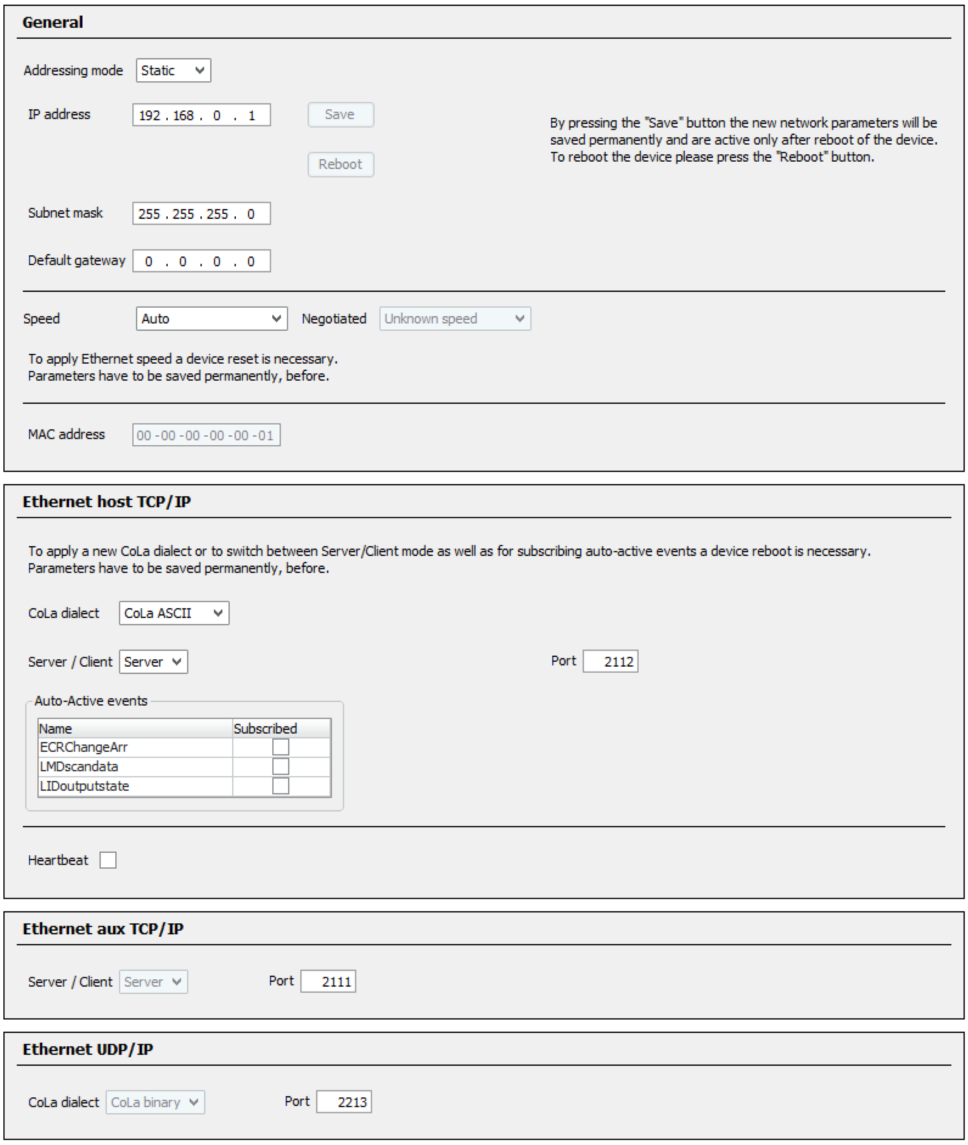
Change default IP address to non-default values.

Limit the subnet mask 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 many 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.

Login as Service.

- ▶ Parameter > Network / Interfaces / IOs > Ethernet



General

Addressing mode: Static

IP address: 192 . 168 . 0 . 1

Save

Reboot

By pressing the "Save" button the new network parameters will be saved permanently and are active only after reboot of the device. To reboot the device please press the "Reboot" button.

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 0 . 0 . 0 . 0

Speed: Auto — Negotiated: Unknown speed

To apply Ethernet speed a device reset is necessary.
Parameters have to be saved permanently, before.

MAC address: 00 -00 -00 -00 -00 -01

Ethernet host TCP/IP

To apply a new CoLa dialect or to switch between Server/Client mode as well as for subscribing auto-active events a device reboot is necessary.
Parameters have to be saved permanently, before.

CoLa dialect: CoLa ASCII

Server / Client: Server — Port: 2112

Auto-Active events

Name	Subscribed
ECRChangeArr	□
LMDscandata	□
LIDoutputstate	□

Heartbeat □

Ethernet aux TCP/IP

Server / Client: Server — Port: 2111

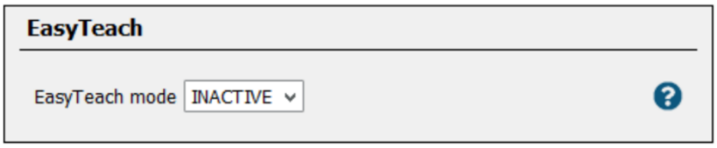
Ethernet UDP/IP

CoLa dialect: CoLa binary — Port: 2213

3.3.3 Deactivate EasyTeach

Set EasyTeach mode to “INACTIVE”

- ▶ Parameter > Evaluation Fields



EasyTeach

EasyTeach mode: INACTIVE

4 Application related recommendations

4.1 Streaming

The LMS5xx provides the distance measurement data as raw data for customer applications. To increase the security and integrity of the measurement data we propose the following security measures.

Remark:

For requesting data from LMS5xx, please refer to publication “Telegram listing”.

4.1.1 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: `SCdevicestate`

Remark:

The status of the measurement function of LMS5xx can be read separately with the telegram `STlms` (status and time).

4.1.2 Scan counter

Missed measurement data can be detect by checking the continuously counting scan counter, which is part of each measurement data telegram `LMDscandata`.

4.1.3 Telegram counter

Telegram counter information is part of `LMDscandata`.

Telegram counter includes the number of measurement telegrams finished in the scanner and given to the interface.

Remark:

Does not count how many telegrams were really given out; is relevant if not all scans are delivered from the scan core. For example, the telegram counter can be used as a plausibility check.

4.1.4 Time stamp

Time stamp information is part of `LMDscandata`.

- Time since start up in µs:

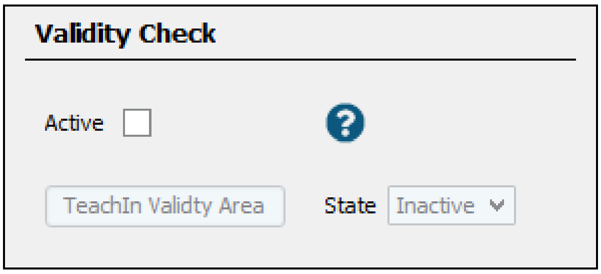
  Counting the time since power up the device; starting with zero. In the output telegram, this is the time at the zero index before the measurement itself starts.
- Time of transmission in µs:

  Time in µs when the complete scan is transmitted to the buffer for data output; starting with zero at scanner bootup.

4.1.5 Plausibility check on measurement data and RSSI values

To get a plausibility check on measurement data and RSSI values, you can use the Validity check. Also possible is to observe an additional reference target, by reading distance and RSSI value of this test target.

▶ Parameter > Security



Validity Check

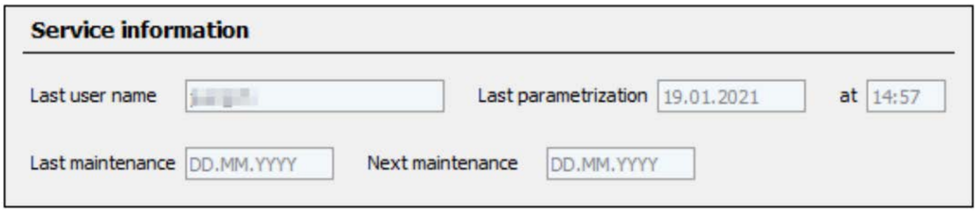
Active ☐

State Inactive

4.2 Recommended Security measures

4.2.1 Last Modified

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



Service information

Last user name	[redacted]	Last parametrization	19.01.2021	at	14:57
Last maintenance	DD.MM.YYYY	Next maintenance	DD.MM.YYYY		

4.2.2 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).

8028850/ / 2023-08-01

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 ertekesites@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

SICK
Sensor Intelligence.