

Cybersecurity

MLG-2



Contents

1	About this document.....	4
1.1	Purpose of this document.....	4
1.2	Scope.....	4
1.3	Target group.....	4
1.4	Further information.....	4
1.5	Related applicable documents.....	5
1.6	Symbols and document conventions.....	5
2	Safety information.....	7
2.1	Basic safety instructions.....	7
2.2	Intended use.....	7
2.3	Qualification of personnel.....	7
3	General information on cybersecurity.....	8
3.1	Cybersecurity threats.....	8
3.2	Cyber resilience.....	9
3.3	Organizational measures at SICK for cybersecurity in products.....	10
4	Product description.....	11
4.1	Product identification via the SICK product ID.....	11
4.2	Product identification via the IO-Link interface.....	11
5	Preventive measures for cybersecurity.....	12
5.1	Check the integrity of downloaded files.....	12
5.2	Updates.....	12
5.3	Access control for network-compatible products.....	12
5.4	Deactivate unused services, protocols and ports.....	12
5.5	Access control for IO-Link devices.....	13
5.6	Limited use of the IO-Link interface.....	13
5.7	Requirements for IO-Link Masters used.....	13
5.8	Protect network from unauthorized access.....	14
5.9	Monitor network traffic.....	14
5.10	Encrypted communication.....	14
5.11	No data transmission to third parties.....	14
5.12	Restrict physical access.....	14
5.13	Backup copy of the configuration.....	15
5.14	Have spare devices ready.....	15
6	Dealing with disruptions.....	16
6.1	Defect.....	16
6.2	Cyber attack.....	16
6.3	Forgotten password.....	16
7	Decommissioning.....	17
7.1	Device replacement and decommissioning.....	17

8	Technical data.....	18
8.1	Communication services.....	18
9	Annex.....	19
9.1	Conformities and certificates.....	19
9.2	Declaration of completeness.....	19

1 About this document

1.1 Purpose of this document

This document contains information on the cybersecurity of the product.

The implementation details of the system environment into which these products are integrated are not part of this document.

This document applies in addition to the other applicable documents such as the operating instructions. The applicable documents must be observed throughout the entire life cycle of the product.

1.2 Scope

This document applies to the following products:

MLG-2 Pro

MLG-2 ProNet

1.3 Target group

This document is intended for persons who are responsible for cybersecurity when using the product.

1.4 Further information

You can find the product page with further information via the SICK Product ID:

pid.sick.com/{P/N}/{S/N}

(see "Product identification via the SICK product ID", page 11).

The following information is available depending on the product:

- This document in all available language versions
- Data sheets
- Other publications
- CAD files and dimensional drawings
- Certificates (e.g., declaration of conformity)
- Software
- Accessories

1.5 Related applicable documents

Related applicable documents from SICK

Table 1: Related applicable documents from SICK

Document	Title	Part number	Source
Operating instructions	Measuring automation light grid	8016616	www.sick.com/8016616
	Measuring automation light grid with EtherCAT® fieldbus	8018739	www.sick.com/8018739
	Measuring automation light grid with EtherNet/IP™ fieldbus	8018741	www.sick.com/8018741
	Measuring automation light grid with CANopen® fieldbus	8018743	www.sick.com/8018743
	Measuring automation light grid with PROFINET fieldbus	8018745	www.sick.com/8018745
	Measuring automation light grid with PROFIBUS fieldbus	8018747	www.sick.com/8018747
	SOPAS ET Manual	-	"help" folder in the locally installed SOPAS ET
Technical information	SICK Smart Sensors/IO-Link	8021939	www.sick.com/8021939

1.6 Symbols and document conventions

Warnings and other notes



DANGER

Indicates a situation presenting imminent danger, which will lead to death or serious injuries if not prevented.



WARNING

Indicates a situation presenting possible danger, which may lead to death or serious injuries if not prevented.



CAUTION

Indicates a situation presenting possible danger, which may lead to moderate or minor injuries if not prevented.



NOTICE

Indicates a situation presenting possible danger, which may lead to property damage if not prevented.



NOTE

Highlights useful tips and recommendations as well as information for efficient and trouble-free operation.

Instructions to action

- The arrow denotes instructions to action.

1. The sequence of instructions is numbered.
2. Follow the order in which the numbered instructions are given.
- ✓ The tick denotes the results of an action.

2 Safety information

2.1 Basic safety instructions

Information on avoiding health hazards and dangerous situations can be found in the relevant operating instructions.

2.2 Intended use

The respective operating instructions and this document together describe the intended use and the cybersecurity-relevant information on the product.

The product is designed for data exchange via interfaces.

The data that is exchanged includes configuration data, diagnostic data, data resulting from the sensor function of the product and data that controls the sensor.

The product is not intended to store personal data.

The product includes functions that can help protect against cybersecurity threats. The use of these functions and the implementation of further measures to protect against cybersecurity threats are the responsibility of the machine manufacturer and the machine operator.

The product is not intended for access control applications.

Incorrect use, improper modification or manipulation of the product will invalidate any warranty from SICK; in addition, any responsibility and liability of SICK for damage and secondary damage caused by this is excluded.

2.3 Qualification of personnel

Any work on the product may only be carried out by personnel qualified and authorized to do so.

Qualified personnel are able to perform tasks assigned to them and can independently recognize and avoid any potential hazards. This requires, for example:

- technical training
- experience
- knowledge of the applicable regulations and standards

3 General information on cybersecurity

3.1 Cybersecurity threats

Overview

To protect against cybersecurity threats, it is necessary to continuously monitor and maintain a comprehensive cybersecurity concept. A suitable concept consists of organizational, technical, procedural, electronic, and physical levels of defense and considers suitable measures for different types of risks. The measures implemented in this product can only support protection against cybersecurity threats if the product is used as part of such a concept.

Threats that the product helps to reduce

Table 2: Threats that the product helps to reduce

Threat	Countermeasures
Denial-of-Service attacks	- Defined behavior with high grid load - Automatic re-establishment of connections
Access to unused protocols and services	Option to deactivate protocols and services
- Write access to devices, settings and data by unauthorized persons - Unauthorized changes to the configuration of the product	- User groups with different rights and passwords - Each user group can be activated and deactivated individually - Ability to save verified configurations and transfer them to the same device or to a replacement device - Checksums to secure the configuration - Option to save configurations via the Data Storage function of the IO-Link protocol and transfer them to the same device or to a replacement device - Use of an existing Device Access Locks function to restrict unauthorized access to physical control elements
Brute-Force attacks	After five invalid login attempts, subsequent login attempts are rejected for a period of 30 seconds, even if they are entered correctly.

Threats that machine manufacturers and machine operators must consider reducing during integration and operation

Table 3: Threats that machine manufacturers and machine operators must consider reducing during integration and operation

Threat	Countermeasures	Affects	Further topics
- Write access to devices, settings and data by unauthorized persons - Excessive write accesses that lead to the destruction of a memory bank (EEPROM/FLASH).	- Use user groups with different rights and passwords - Deactivate unneeded user groups - Change initial passwords - Use secure passwords - Change passwords regularly and when necessary, e.g. if a cybersecurity incident is suspected - Use a suitable port configuration	- Product when using the Ethernet interface - IO-Link Master when using IO-Link	- see "Access control for network-compatible products", page 12 - see "Deactivate unused services, protocols and ports", page 12 - see "Requirements for IO-Link Masters used", page 13 - see "Access control for IO-Link devices", page 13 - see "Deactivate unused services, protocols and ports", page 12

Threat	Countermeasures	Affects	Further topics
- Remote access by unauthorized persons - Access to unused protocols and services	- Deactivate unused interfaces, protocols and services - Protect network from unauthorized access - Use SIO mode (IO-Link only)	- Product when using the Ethernet interface - IO-Link Master when using IO-Link	- see "Limited use of the IO-Link interface", page 13 - see "Deactivate unused services, protocols and ports", page 12 - see "Requirements for IO-Link Masters used", page 13 - see "Deactivate unused services, protocols and ports", page 12
- Physical access to devices by unauthorized persons Social Engineeringi.e. unauthorized persons gain the trust of authorized persons	- Physically restrict access - Take organizational measures - Promoting awareness among the workforce	- Product when using the Ethernet interface - IO-Link Master when using IO-Link	see "Restrict physical access", page 14
Denial-of-Service attacks	- Defined behavior with high mains load (in IO-Link Master) - Automatic re-establishment of connections (in IO-Link Master)	IO-Link Master when using IO-Link	see "Requirements for IO-Link Masters used", page 13
Unauthorized changes to the configuration of the product	- Saving the configuration - Use of the data storage function (IO-Link only) - Suitable port configuration	- Product when using the Ethernet interface - IO-Link Master when using IO-Link	- see "Deactivate unused services, protocols and ports", page 12 - see "Backup copy of the configuration", page 15 - see "Requirements for IO-Link Masters used", page 13

3.2 Cyber resilience

Overview

Despite all defensive measures, unauthorized persons can still succeed in compromising the system. Provision should be made for this eventuality.

Precautionary measures

Suitable precautionary measures should be taken for the entire system environment so that the system environment can be put back into operation as quickly as possible after an incident.

Several backup copies of the entire configuration should be made for the product.

Further topics

- see ["Backup copy of the configuration"](#), page 15

3.3 Organizational measures at SICK for cybersecurity in products

Product design

SICK develops new products in accordance with **SICK Security Development Lifecycle**, which covers the entire life cycle of a product (product development, operation and maintenance, de-commissioning). The basic version of **SICK Security Development Lifecycle** implements basic cybersecurity requirements. The full version of the **SICK Security Development Lifecycle** is certified in accordance with IEC 62443-4-1.

The product was developed before the completion of the **SICK Security Development Lifecycle**. Nevertheless, it meets the central requirements of **SICK Security Development Lifecycle**.

Vulnerability management

At SICK, a dedicated **Product Incident Response Team (PSIRT)** is responsible for reports and questions about cybersecurity. Under www.sick.com/psirt you will find further information and measures for published vulnerabilities.

Contact

If you have any questions or if a cybersecurity incident has occurred, please contact psirt@sick.de.

4 Product description

4.1 Product identification via the SICK product ID

SICK product ID

The SICK product ID uniquely identifies the product. It also serves as the address of the web page with information on the product.

The SICK product ID comprises the host name pid.sick.com, the part number (P/N), and the serial number (S/N), each separated by a forward slash.

For many products, the SICK product ID is displayed as text and QR code on the type label and/or on the packaging.



Figure 1: SICK product ID

4.2 Product identification via the IO-Link interface

The **SICK Product ID** can be read out via the IO-Link interface of the device.

IO-Link service data is used for this purpose:

Table 4: IO-Link service data for product identification

ISDU			Name	Notes
Index		Subindex		
DEC	HEX			
19	13	-	Product ID	Product ID contains the part number (P/N) of the product. Older products may contain the note "see Index 219". In this case, index 219 / subindex 0 must be used.
219	DB	1	Product ID IO-Link Device	Used for older products. Product ID IO-Link Device contains the part number (P/N) of the product.
21	15	-	Serial Number	Serial Number contains the serial number (S/N) of the product.
27	1B	-	Product URI	Only for newer products: Product URI contains the full text of SICK Produkt ID, i.e. "pid.sick.com/{P/N}/{S/N}".

5 Preventive measures for cybersecurity

5.1 Check the integrity of downloaded files

The corresponding SHA-256 hash value is specified for each download on the SICK website. After downloading, the integrity of the downloaded file can be checked using the SHA-256 hash value. Information on the procedure can be found at www.sick.com/verify-downloads.

5.2 Updates

Please contact support to rectify any product vulnerabilities that have become known. If necessary, the manufacturer will update the product firmware or replace the product.

5.3 Access control for network-compatible products

Overview

The devices contain a hierarchy of user groups that regulate access to the devices.

For certain actions (e.g. transferring a configuration to the device), you will be prompted to log in to the device with the corresponding user group.

Further information on the user groups can be found in the operating instructions for the respective product in the section "Configuration with SOPAS ET - Operating SOPAS ET - User level".



NOTE

- Change initial passwords to prevent unauthorized access.
- Deactivate unused user groups.

Password transfer

Registration on the device is carried out using a **Challenge-Response** procedure. For transmission, a hash value is determined using the SHA-256 algorithm.

Change and reset passwords

Information on how to change and reset passwords can be found in the operating instructions for the respective product in the section "Configuration with SOPAS ET - Operation SOPAS ET - User level".

When a password is changed, the new password is transmitted in encrypted form. If there is a suspicion that the old password has become known to unauthorized persons, the new password should be assigned via a trusted connection (e.g. secured network).

5.4 Deactivate unused services, protocols and ports

Interfaces, services and ports

Information on the physical interfaces can be found in the operating instructions of the respective product in the section "For your safety - Cybersecurity".

An overview of the network services provided and the associated ports can be found in the operating instructions for the respective product in the sections "Configuration with SOPAS ET - Operation SOPAS ET - Service settings (service user level)" and "Technical data - Data sheet".

Information on deactivating other interfaces (I/Os, RS485...) can be found in the operating instructions for the respective product in the section "Configuration with SOPAS ET - Operation SOPAS ET - System settings - System settings for the EXPERT function level - I/O configuration"

Deactivate unused interfaces and services

It is recommended to deactivate unused interfaces and services. Further information can be found in the operating instructions for the respective product in the sections "Configuration with SOPAS ET - Operating SOPAS ET - Service settings (service user level)" and "Configuration with SOPAS ET - Operating SOPAS ET - System settings - System settings for the EXPERT function level - I/O configuration".

5.5 Access control for IO-Link devices

Overview

The devices do not contain any customer-accessible authentication options. The IO-Link interface on the product allows random read or write access without access control in accordance with the specification.

Cybersecurity threats due to access to the device can only be reduced by taking measures in the downstream assemblies of the product, in particular the IO-Link Master.

Device Access Locks

Existing physical control elements on the product (teach-in buttons, digital input lines, etc.) can be locked using the **Device Access Locks** IO-Link function. Details can be found in the operating instructions for the product.

Service functions

The product contains service functions that cannot be switched off, which the manufacturer can use via IO-Link. These functions include the option for the manufacturer to import firmware updates or to check and revise production settings.

5.6 Limited use of the IO-Link interface

Only use the IO-Link interface if necessary.

If IO-Link is only required to (re-)configure the product, it is advisable to use SIO mode during operation and thus switch off all digital communication with the product. Two system configurations with different levels of risk can be used:

- Operation of the product on a digital I/O assembly without IO-Link function. This system configuration offers the highest level of protection against cybersecurity threats, as there is no possibility of accessing the product via IO-Link.
- Configuration of the IO-Link port as a digital input or output on an IO-Link Master. This system configuration does not allow access to the product via IO-Link as long as access to the port configuration of the IO-Link Master is sufficiently secured.

5.7 Requirements for IO-Link Masters used

This section documents requirements for an IO-Link Master that is connected to the product. Meeting these requirements reduces cybersecurity threats to the product.

As a threat model, the requirements assume that the IO-Link Master is connected to higher-level assemblies via a routable wired network (e.g. Ethernet). If the interface architecture differs from this (especially cable-free interfaces), additional measures may be necessary to reduce cybersecurity threats.

Alternatives to these requirements are conceivable, e.g. through superimposed assemblies or network structures. The machine manufacturer and the machine operator are responsible for designing and testing the effectiveness of these alternative requirements.

5.8 Protect network from unauthorized access

Restrict network access

Only authorized communication partners should have access to the local network.

In many cases, remote access is required for service technicians to carry out maintenance work remotely. To prevent such remote access paths from being exploited for unauthorized access, they must be specially protected. If the local network in which the IO-Link Master connected to the product is located is connected to other networks, the transition should be secured by a firewall, for example. Remote access can take place via an encrypted VPN (virtual private network), for example.

Firewall settings

Depending on the services that are to be accessible through the firewall, the corresponding ports for the respective IP address of the IO-Link Master connected to the product must be enabled in the firewall.

An overview of the network services provided and the associated ports can be found in the operating instructions for the connected IO-Link Master.

5.9 Monitor network traffic

The data traffic in the network of the IO-Link Master connected to the product should be continuously monitored so that failures, anomalies and attacks are detected at an early stage.

5.10 Encrypted communication

If unencrypted data is transmitted in a network, other network participants can read and manipulate this data. If unauthorized persons gain access to the network, they can use unencrypted data connections for attacks.

Data connections should therefore always be encrypted if possible. Data transmission between the local network in which the IO-Link Master connected to the product is located and devices outside of this network can occur via an encrypted VPN, for example.

A VPN (**Virtual Private Network**) connects networks or network-capable devices via a public network, e.g., via the Internet. The data transmission should always be encrypted. This is generally the case with current VPN technologies.

5.11 No data transmission to third parties

The product does not transmit any data other than that specified in the configuration. The product itself does not transmit any data to SICK or third parties.

5.12 Restrict physical access

Physical access to the product makes it easier for unauthorized persons to access data or the network. Therefore, only authorized persons should have access to the product.

Depending on the operating environment, different restrictions of access are possible, e.g.:

- Laying protected cables
- Install product firmly in machine or vehicle
- Restricted access to the rooms in which the product is operated
- Attach seals or similar to pin connectors on the product in order to be able to detect unauthorized attached cables

These specifications also apply analogously to a connected IO-Link Master.

5.13 Backup copy of the configuration

It is recommended to make backup copies of the entire configuration. To do this, the **Data Storage** function of a connected IO-Link Master should be activated. The IO-Link Master should offer the function of downloading the **data storage** data ("BLOB") to a connected service PC or similar.

If the product needs to be replaced or the configuration has been changed, for example by manipulation, a backup copy of the configuration can be transferred to the same device or to a replacement device.

The following points should be taken into account for the backup copies:

- Several backup copies should be stored separately.
- The process for transferring the backup copy to the device should be tested.
- Backup copies should always be up-to-date. If the configuration is changed, a new backup copy should be created. Each new backup copy should be tested to ensure that it can be transferred to the device.
- Together with the backup copy, the configuration program should be saved in the current version so that it is available at any time to transfer the backup copy to the device.
- Backup copies should be stored on permanently readable data cards.
- Backup copies should be protected against network access and other accesses so that unauthorized persons cannot delete or change them.
- Backup copies should be protected with a password. The password cannot be reset. If the password is lost, the project file has to be created again.
- Backup copies should be protected against burglary, fire, water, etc.

Additional information on saving a configuration can be found in the operating instructions for the IO-Link Master connected to the product.

5.14 Have spare devices ready

It is recommended to have spare devices ready. In the event of a defect or if there is a possibility that a product has been compromised following a cyber attack, you can replace the product and transfer a backup copy.

6 Dealing with disruptions

6.1 Defect

If the device is defective, it must be replaced. You can transfer a backup copy of the configuration to the new device, [see "Backup copy of the configuration", page 15](#).



NOTE

After transferring the configuration to a new device, it may be necessary to teach in individual configuration elements again (so-called "teach-in"). Observe the operating instructions for the product.

6.2 Cyber attack

If you are unsure whether the product has been compromised after a cyber attack, contact your local SICK subsidiary.

6.3 Forgotten password

Information on resetting passwords can be found in the operating instructions for the respective product in the section "Configuration with SOPAS ET - Operation SOPAS ET - User level".

7 Decommissioning

7.1 Device replacement and decommissioning

Device replacement

If the device is defective, it must be replaced. You can transfer a backup copy of the configuration to the new device, [see "Backup copy of the configuration", page 15](#).

De-commissioning

When decommissioning the device, it should be reset to the factory settings. This overwrites the saved passwords, among other things.

Information on resetting to factory settings can be found in the operating instructions for the respective product in the section "Configuration with SOPAS ET - Operation SOPAS ET - System settings for the EXPERT function level".

8 Technical data

8.1 Communication services

An overview of the network services provided and the associated ports as well as the protocols and ports via which SOPAS ET communicates can be found in the operating instructions for the respective product in the sections "Configuration with SOPAS ET - Operation SOPAS ET - Service settings (service user level)" and "Technical data - Data sheet".

9 Annex

9.1 Conformities and certificates

You can obtain declarations of conformity, certificates, and the current operating instructions for the product at www.sick.com. To do so, enter the product part number in the search field (part number: see the entry in the “P/N” or “Ident. no.” field on the type label).

9.2 Declaration of completeness

All interfaces of the product are described to the best of our knowledge in the operating instructions of the respective product. No interface was intentionally omitted.

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) 30 204 40 00
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

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

Detailed addresses and further locations at www.sick.com

