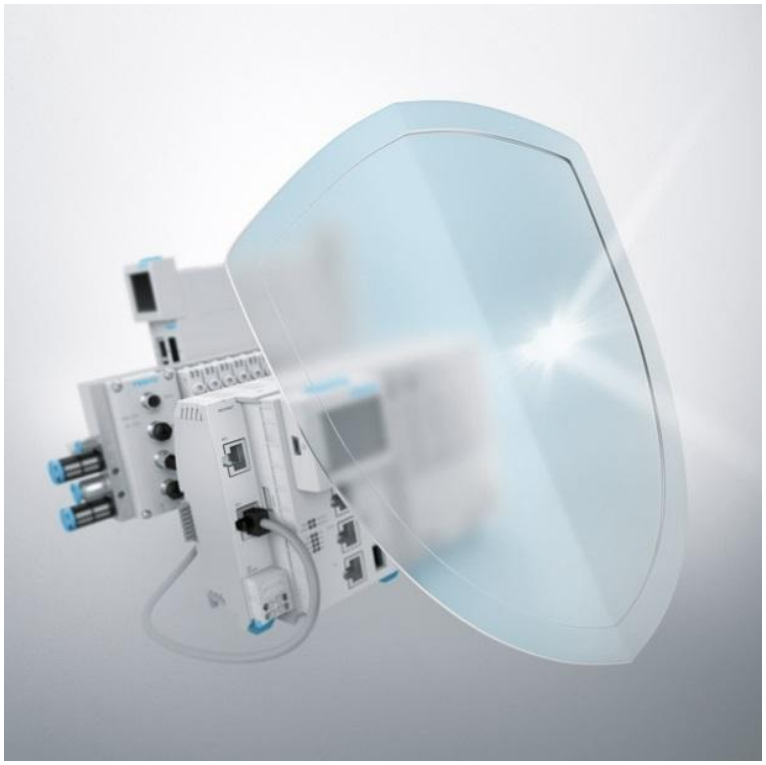
Vulnerability in Ethernet/IP Stack of SBRD-Q/SBOC-Q/SBOI-Q



FSA-202101

Date
January 11th, 2024

Creator
Festo SE & Co. KG

Version
1.0.1

Festo SE & Co. KG

www.festo.com/psirt
psirt@festo.com
Ruiter Straße 82
73734 Esslingen
GERMANY

Summary

Festo products for machine vision are affected by multiple vulnerabilities.
The affected product families are cameras SBOC-Q/SBOI-Q and the Controller SBRD-Q.
The vulnerabilities are all in the Ethernet IP Stack from EIPStackGroup OpENer Ethernet/IP.

Vulnerability Identifier

IDs: ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP
CVEs: CVE-2021-27478, CVE-2021-27482, CVE-2021-27498, CVE-2021-27500

Severity

8.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)

Affected Vendors

FESTO

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
SBOC-Q-R1B: Firmware all Versions affected	Festo:Partnumber:541399 Festo:Ordercode:SBOC-Q-R1B	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device

Affected Product and Versions	Product Details	Remediation
		settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R1B-S1: Firmware all Versions affected	Festo:Partnumber: 569771 Festo:Ordercode:SBOC-Q-R1B-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R1C: Firmware all Versions affected	Festo:Partnumber: 548317 Festo:Ordercode:SBOC-Q-R1C	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.

Affected Product and Versions	Product Details	Remediation
SBOC-Q-R1C-S1: Firmware all Versions affected	Festo:Partnumber: 569774 Festo:Ordercode:SBOC-Q-R1C-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R3B-WB: Firmware all Versions affected	Festo:Partnumber: 555841 Festo:Ordercode:SBOC-Q-R3B-WB	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R3B-WB-S1: Firmware all	Festo:Partnumber: 569777	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices

Affected Product and Versions	Product Details	Remediation
Versions affected	Festo:Ordercode:SBOC-Q-R3B-WB-S1	and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R3C-WB: Firmware all Versions affected	Festo:Partnumber: 555842 Festo:Ordercode:SBOC-Q-R3C-WB	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R3C-WB-S1: Firmware all Versions affected	Festo:Partnumber: 569778 Festo:Ordercode:SBOC-Q-R3C-WB-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations.

Affected Product and Versions	Product Details	Remediation
		For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R2B: Firmware all Versions affected	Festo:Partnumber: 551021 Festo:Ordercode:SBOC-Q-R2B	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R2B-S1: Firmware all Versions affected	Festo:Partnumber: 569772 Festo:Ordercode:SBOC-Q-R2B-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS

Affected Product and Versions	Product Details	Remediation
		Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOC-Q-R2C: Firmware all Versions affected	Festo:Partnumber: 551022 Festo:Ordercode:SBOC-Q-R2C	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R1B: Firmware all Versions affected	Festo:Partnumber: 541396 Festo:Ordercode:SBOI-Q-R1B	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP:

Affected Product and Versions	Product Details	Remediation
		Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R1B-S1: Firmware all Versions affected	Festo:Partnumber: 569773 Festo:Ordercode:SBOI-Q-R1B-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R1C: Firmware all Versions affected	Festo:Partnumber: 548316 Festo:Ordercode:SBOI-Q-R1C	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device

Affected Product and Versions	Product Details	Remediation
		settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R1C-S1: Firmware all Versions affected	Festo:Partnumber: 569776 Festo:Ordercode:SBOI-Q-R1C-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R3B-WB: Firmware all Versions affected	Festo:Partnumber: 555839 Festo:Ordercode:SBOI-Q-R3B-WB	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.

Affected Product and Versions	Product Details	Remediation
SBOI-Q-R3B-WB-S1: Firmware all Versions affected	Festo:Partnumber: 569779 Festo:Ordercode:SBOI-Q-R3B-WB-S1	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R3C-WB: Firmware all Versions affected	Festo:Partnumber: 555840 Festo:Ordercode:SBOI-Q-R3C-WB	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBOI-Q-R3C-WB-S1: Firmware all	Festo:Partnumber: 569780	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices

Affected Product and Versions	Product Details	Remediation
Versions affected	Festo:Ordercode:SBOI-Q-R3C-WB-S1	and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.
SBRD-Q: Firmware all Versions affected	Festo:Partnumber: 8067301 Festo:Ordercode:SBRD-Q	For CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. See section Workarounds and Mitigations. For CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP, CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP: Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. Deactivate EtherNet/IP in device settings if not used. See section Workarounds and Mitigations.

Workarounds and Mitigations

Remediations can be found in the table of Affected Products and Recommendations.

Additionally, please refer to the General Recommendations.

Impact and Classification of Vulnerabilities

CVE-2021-27478, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP
A specifically crafted packet sent by an attacker to the affected devices may cause a denial-of-service condition.
Weakness: Incorrect Conversion between Numeric Types (CWE-681)
Base Score: 8.2
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
CVE-2021-27482, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP
A specifically crafted packet sent by an attacker may allow the attacker to read arbitrary data.
Weakness: Out-of-bounds Read (CWE-125)
Base Score: 7.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2021-27498, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP
A specifically crafted packet sent by an attacker to the affected devices may cause a denial-of-service condition.
Weakness: Reachable Assertion (CWE-617)
Base Score: 7.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2021-27500, ICS Advisory (ICSA-21-105-02) EIPStackGroup OpENer Ethernet/IP
A specifically crafted packet sent by an attacker to the affected devices may cause a denial-of-service condition.
Weakness: Reachable Assertion (CWE-617)
Base Score: 7.5
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

General recommendations

Festo strongly recommends to minimize and protect network access to connected devices with state of the art techniques and processes.
For a secure operation follow the recommendations in the product manuals.

Acknowledgments

Festo SE & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination and support with this publication (see: https://cert.vde.com/)

Publisher Details

https://festo.com
Festo SE & Co. KG PSIRT Ruiter Straße 82 73734 Esslingen Germany, psirt@festo.com

Include further information here

Further References

For further information also refer to:

- VDE-2021-045

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	September 22nd, 2021	Initial version
1.0.1	January 11th, 2024	Adjust link to VDE Advisory

Sharing rules

TLP: WHITE
For the TLP version see: https://www.first.org/tlp

Disclaimer

Festo assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided free of charge and on good faith by Festo. Insofar as permissible by law, however, none of this information shall establish any warranty, guarantee, commitment or liability on the part of Festo. Note: In no case does these information release the operator or responsible person from the obligation to check the effect on his system or installation before using the information and, in the event of negative consequences, not to use the information.

In addition, the actual general terms and conditions of Festo for delivery, payment and software use shall apply, available under http://www.festo.com.