

product type designation

SFP992-1BX10T

SCALANCE X accessory; Plug-in transceiver SFP992-1BX10T; 1x 1000 Mbit/s LC port, optical; single-mode optical up to max. 10 km BiDi Transceiver 1550 nm/1310 nm.



interfaces	
number of electrical/optical connections / for network components or terminal equipment / maximum	1
number of optical interfaces / for network components or terminal equipment / maximum	1
number of 1000 Mbit/s LC ports / for single mode (LD) / integrated	1
design of the optical interface / for network components or terminal equipment	LC
wavelength / of the optical interface	1550 nm; Single-mode
connectable optical power relative to 1 mW	
<ul style="list-style-type: none"> of the transmitter output / minimum of the transmitter output / maximum of the receiver input / maximum 	-9 dB -3 dB -3 dB
optical sensitivity relating to 1 mW / of the receiver input / minimum	-21 dB
attenuation factor / of the FOC transmission link / minimum necessary	0 dB
range / at the optical interface / depending on the optical fiber used	0 ... 10 km
transmission method / for connection type 1	1000BASE-BX
ambient conditions	
ambient temperature	
<ul style="list-style-type: none"> during operation during storage during transport 	-40 ... +85 °C -40 ... +85 °C -40 ... +85 °C
relative humidity / at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP20
design, dimensions and weights	
design	SFP Module
width	14 mm
height	9 mm
depth	57 mm
net weight	0.02 kg
fastening method	latched
standards, specifications, approvals	
standard	
<ul style="list-style-type: none"> for hazardous zone for safety / from CSA and UL for emitted interference 	EN 60079-0: 2011, EN60079-15: 2010, II 3 G Ex nA II T4, KEMA 07 ATEX 0145 X UL 62368-1 and CAN/CSA C22.2 No. 62368-1:19 EN 61000-6-4:2007 (Class A)

<ul style="list-style-type: none"> for interference immunity 	EN 61000-6-2:2005
certificate of suitability	EN 61000-6-2:2005, EN 61000-6-4:2007
<ul style="list-style-type: none"> CE marking 	Yes
<ul style="list-style-type: none"> C-Tick 	Yes
<ul style="list-style-type: none"> KC approval 	No
<ul style="list-style-type: none"> CCC / for hazardous zone according to GB standard 	Yes; GB3836.1, GB3836.8
<ul style="list-style-type: none"> CCC / for hazardous zone according to GB standard / as marking 	Ex nA IIC T4 Gc
MTBF	320 a
reference code	KEC
<ul style="list-style-type: none"> according to IEC 81346-2:2019 	KEC

standards, specifications, approvals / Environmental Product Declaration

Environmental Product Declaration	Yes
global warming potential [CO2 eq]	
<ul style="list-style-type: none"> total 	16.27 kg
<ul style="list-style-type: none"> during manufacturing 	1.7 kg
<ul style="list-style-type: none"> during operation 	14.56 kg
<ul style="list-style-type: none"> after end of life 	0.01 kg

further information / internet links

internet link	
<ul style="list-style-type: none"> to website: Selection guide for cables and connectors 	https://support.industry.siemens.com/cs/ww/en/view/109766358
<ul style="list-style-type: none"> to web page: selection aid TIA Selection Tool 	https://www.siemens.com/tstcloud
<ul style="list-style-type: none"> to website: Industrial communication 	https://www.siemens.com/simatic-net
<ul style="list-style-type: none"> to web page: SiePortal 	https://sieportal.siemens.com/
<ul style="list-style-type: none"> to website: Image database 	https://www.automation.siemens.com/bilddb
<ul style="list-style-type: none"> to website: CAx-Download-Manager 	https://www.siemens.com/cax
<ul style="list-style-type: none"> to website: Industry Online Support 	https://support.industry.siemens.com

security information

security information	<p>Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)</p>
----------------------	---

Approvals / Certificates

General Product Approval	For use in hazardous locations
--------------------------	--------------------------------



EG-Konf.



IECEX



ATEX

[FM](#)

For use in hazardous locations	Environment
--------------------------------	-------------

[CCC-Ex](#)



last modified:

9/13/2025