

product type designation	RUGGEDCOM SFP1112-1I RUGGEDCOM Accessory, Copper SFP, 1x 10/100/1000MBIT/S, RJ45-Interface, Copper: Up to max. 100m, -40...+85 Degrees Celsius. For use with ROS 5.4.0, ROX 2.13.2 and later versions.
suitability for operation	compatible to RUGGEDCOM products with SFP-Slot
interfaces	
number of electrical/optical connections / for network components or terminal equipment / maximum	1
number of electrical connections <ul style="list-style-type: none"> for network components or terminal equipment / maximum 	1
number of 10/100/1000 Mbit/s RJ45 ports	1
type of electrical connection <ul style="list-style-type: none"> for network components or terminal equipment 	RJ45
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
design, dimensions and weights	
design	SFP Module
width	14 mm
height	12 mm
depth	57 mm
net weight	0.01 kg
fastening method	latched
standards, specifications, approvals	
standard <ul style="list-style-type: none"> for safety / from CSA and UL for emitted interference for interference immunity 	standard / for safety / from CSA and UL EN 61000-6-4 (Class A) EN 61000-6-2
laser protection class	Complies with 21 CFR chapter 1, subchapter J
certificate of suitability <ul style="list-style-type: none"> CE marking C-Tick KC approval IEC 61850-3 	EN 61000-6-2, EN 61000-6-10 Yes Yes No Yes
further information / internet links	
internet link <ul style="list-style-type: none"> to website: Image database to website: CAx-Download-Manager to website: Industry Online Support 	https://www.automation.siemens.com/bilddb http://www.siemens.com/cax https://support.industry.siemens.com
security information	
security information	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)

Approvals / Certificates

General Product Approval

other



[inspection certificate](#)

last modified:

4/19/2024 