SIEMENS

Data sheet 6GK6000-8CG01-0AA0

product type designation	**RUGGEDCOM SFP1112-1**
	RUGGEDCOM Accessory, Copper SF P, 1 X 10/100/1000MBIT/S, RJ45 =-Interface, Copper: Up to max. 100m, 0...+70 Degrees Celcius
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	
● for network components or terminal equipment / maximum	1
number of 10/100/1000 Mbit/s RJ45 ports	1
type of electrical connection	
● for network components or terminal equipment	RJ45
ambient conditions	
ambient temperature	
● during operation	0 ... 70 °C
● during storage	-40 ... +85 °C
● during transport	-40 ... +85 °C
design, dimensions and weights	
design	SFP Module
width	13.7 mm
height	11.9 mm
depth	56.5 mm
net weight	0.01 kg
fastening method	latched
standards, specifications, approvals	
standard	
● for safety / from CSA and UL	UL 60950-1, CSA C22.2 No. 60950-7
● for emitted interference	EN 61000-6-4 (Class A)
● for interference immunity	EN 61000-6-2
laser protection class	Complies with 21 CFR chapter 1, subchapter J
certificate of suitability	EN 61000-6-2, EN 61000-6-10
● CE marking	Yes
● C-Tick	Yes
● KC approval	No
● E1 approval	No
● IEC 61850-3	Yes
further information / internet links	
internet link	
● to website: Image database	https://www.automation.siemens.com/bilddb
● to website: CAx-Download-Manager	http://www.siemens.com/cax
● to website: Industry Online Support	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
Manufacturer Declaration	CE EG-Konf.	inspection certificate

last modified: 4/19/2024