

product type designation	<b>RUGGEDCOM Media Module 1FG02</b>
	Media Module for RUGGEDCOM RSG2100, RSG2100P, RSG2200, and RSG2288, 1 x 1000Mbit/s, SC-interface, Optical: 1000BASE-LX, Single Mode fiber optic up to 10 kilometer, 1300nm (1FG02). Requires the in-field modification kit, 6GK6000-1BC50-0AA1.
Technical Product Detail Page	<a href="https://l.siemens.com/1P6GK6000-8FG02-1AA0">https://l.siemens.com/1P6GK6000-8FG02-1AA0</a>
suitability for operation	RSG2xxx
<b>interfaces</b>	
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 SC ports (LX)	1
design of the optical interface / for network components or terminal equipment	SC
range / at the optical interface / depending on the optical fiber used	10 km
<b>ambient conditions</b>	
ambient temperature	
<ul style="list-style-type: none"> <li>during operation</li> <li>during storage</li> <li>during transport</li> <li>note</li> </ul>	-40 ... +85 °C -40 ... +85 °C -40 ... +85 °C A maximum operating temperature of +85 °C is permissible for a duration of 16 hours
relative humidity / at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP40 (when installed)
<b>design, dimensions and weights</b>	
design	Media module
product feature / conformal coating	No
fastening method	screwed
<ul style="list-style-type: none"> <li>installation in media module slot</li> </ul>	Yes
<b>standards, specifications, approvals</b>	
standard	
<ul style="list-style-type: none"> <li>for EMC</li> <li>for safety / from CSA and UL</li> <li>for hazardous zone / from CSA and UL</li> <li>for emitted interference</li> <li>for interference immunity</li> </ul>	FCC Part 15 (Class A), EN55022 (CISPR22 Class A) UL 60950-1, CSA C22.2 No. 60950-7 Hazardous Locations: Class 1 Division 2 EN 61000-6-4 (Class A) EN 61000-6-2
laser protection class	21 CFR Chapter 1, Subchapter J
certificate of suitability	EN 61000-6-2, EN 61000-6-10
<ul style="list-style-type: none"> <li>CE marking</li> <li>C-Tick</li> <li>KC approval</li> <li>E1 approval</li> <li>IEC 61850-3</li> </ul>	Yes No No No Yes
<b>further information / internet links</b>	
internet link	
<ul style="list-style-type: none"> <li>to website: Selection guide for cables and connectors</li> <li>to website: Industry Mall/RUGGEDCOM selector</li> <li>to website: Industrial communication</li> <li>to website: Siemens RUGGEDCOM</li> <li>to web page: SiePortal</li> </ul>	<a href="https://support.industry.siemens.com/cs/ww/en/view/109766358">https://support.industry.siemens.com/cs/ww/en/view/109766358</a> <a href="https://www.siemens.com/ruggedcom-selector">https://www.siemens.com/ruggedcom-selector</a> <a href="https://www.siemens.com/simatic-net">https://www.siemens.com/simatic-net</a> <a href="https://www.siemens.com/ruggedcom">https://www.siemens.com/ruggedcom</a> <a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a>

- to website: Image database
- to website: CAx-Download-Manager
- to website: Industry Online Support

<https://www.automation.siemens.com/bilddb>

<https://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](http://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](#) [inspection certificate](#)

last modified:

11/14/2025 