

product type designation

**RUGGEDCOM 2488-24FG02 Module CC**

Media Module for RUGGEDCOM RSG 2488, 4 x 1000Mbit/s SC-interface, Optical: 1000BASE-LX, Single Mode fiber optic up to 10 kilometer, 1310nm with Conformal Coating



Figure similar

Technical Product Detail Page

<https://l.siemens.com/1P6GK6000-8FG02-4EA1>

suitability for operation

RSG2488

### interfaces

number of electrical/optical connections / for network components or terminal equipment / maximum	4
number of optical interfaces / for network components or terminal equipment / maximum	4
number of 1000 Mbit/s SC ports (LX)	4
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

### ambient conditions

ambient temperature	
<ul style="list-style-type: none"> <li>during operation</li> <li>during storage</li> <li>during transport</li> <li>note</li> </ul>	<p>-40 ... +85 °C</p> <p>-40 ... +85 °C</p> <p>-40 ... +85 °C</p> <p>A maximum operating temperature of +85 °C is permissible for a duration of 16 hours</p>
relative humidity / at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP40 (when installed)

### design, dimensions and weights

design	Media module
width	110 mm
height	22 mm
depth	91 mm
net weight	0.43 kg
product feature / conformal coating	Yes
fastening method	screwed
<ul style="list-style-type: none"> <li>installation in media module slot</li> </ul>	Yes

### standards, specifications, approvals

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>	<p>FCC Part 15 (Class A), EN55022 (CISPR22 Class A)</p> <p>UL 60950-1, CSA C22.2 No. 60950-7</p> <p>Hazardous Locations: Class 1 Division 2</p> <p>EN 61000-6-4 (Class A)</p> <p>EN 61000-6-2</p>
laser protection class	21 CFR Chapter 1, Subchapter J

certificate of suitability	EN 61000-6-2, EN 61000-6-10
• CE marking	Yes
• C-Tick	No
• KC approval	No
• E1 approval	No
• IEC 61850-3	Yes

**further information / internet links**

internet link	
• to website: Selection guide for cables and connectors	<a href="https://support.industry.siemens.com/cs/ww/en/view/109766358">https://support.industry.siemens.com/cs/ww/en/view/109766358</a>
• to website: Industry Mall/RUGGEDCOM selector	<a href="https://www.siemens.com/ruggedcom-selector">https://www.siemens.com/ruggedcom-selector</a>
• to website: Industrial communication	<a href="https://www.siemens.com/simatic-net">https://www.siemens.com/simatic-net</a>
• to website: Siemens RUGGEDCOM	<a href="https://www.siemens.com/ruggedcom">https://www.siemens.com/ruggedcom</a>
• to web page: SiePortal	<a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a>
• to website: Image database	<a href="https://www.automation.siemens.com/bilddb">https://www.automation.siemens.com/bilddb</a>
• to website: CAx-Download-Manager	<a href="https://www.siemens.com/cax">https://www.siemens.com/cax</a>
• to website: Industry Online Support	<a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>

**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 <a href="http://www.siemens.com/cybersecurity-industry">www.siemens.com/cybersecurity-industry</a> . 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 <a href="https://www.siemens.com/cert">https://www.siemens.com/cert</a> . (V4.7)
----------------------	--

**Approvals / Certificates**

<b>General Product Approval</b>	<b>other</b>
---------------------------------	--------------

[Manufacturer Declaration](#)     [inspection certificate](#)

last modified: 11/14/2025 