

Line Module 4x 10/100/1000TX RJ45

Technical Product Detail Page	<a href="https://i.siemens.com/1P6GK6050-0AL20-0FC0">https://i.siemens.com/1P6GK6050-0AL20-0FC0</a>
suitability for operation	RX5000
<b>interfaces</b>	
number of electrical/optical connections / for network components or terminal equipment / maximum	4
number of electrical connections <ul style="list-style-type: none"> <li>for network components or terminal equipment / maximum</li> </ul>	4
number of 10/100/1000 Mbit/s RJ45 ports	4
type of electrical connection <ul style="list-style-type: none"> <li>for network components or terminal equipment</li> </ul>	RJ45
<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
<b>design, dimensions and weights</b>	
design	Media module
width	40 mm
height	180 mm
depth	240 mm
net weight	1 kg
product feature / conformal coating	No
fastening method <ul style="list-style-type: none"> <li>installation in media module slot</li> </ul>	screwed 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
certificate of suitability <ul style="list-style-type: none"> <li>CE marking</li> <li>C-Tick</li> <li>KC approval</li> <li>E1 approval</li> <li>railway application in accordance with EN 50155</li> <li>railway application in accordance with EN 50124-1</li> <li>IEC 61850-3</li> </ul>	EN 61000-6-2, EN 61000-6-10 Yes No No No Yes Yes 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> </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>

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



- <https://sieportal.siemens.com/>
- <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	Test Certificates	other	Environment
<a href="#">Manufacturer Declaration</a>		<a href="#">inspection certificate</a>	

last modified:

11/14/2025 