SIEMENS

## Data sheet 6GK6000-8CG01-2EA0

| | |
|---|---|
| **product type designation** | **RUGGEDCOM 2488-22CG01 Module** |
| | Media Module for RUGGEDCOM RSG 2488, 2 x RJ45, 10/100/1000BAS E-TX |



| | |
|---|---|
| Technical Product Detail Page | https://i.siemens.com/1P6GK6000-8CG01-2EA0 |
| suitability for operation | RSG2488 |
| **interfaces** | |
| number of electrical/optical connections / for network components or terminal equipment / maximum | 2 |
| number of electrical connections | |
| ● for network components or terminal equipment / maximum | 2 |
| number of 10/100/1000 Mbit/s RJ45 ports | 2 |
| type of electrical connection | |
| ● for network components or terminal equipment | RJ45 |
| **ambient conditions** | |
| ambient temperature | |
| ● during operation | -40 ... +85 °C |
| ● during storage | -40 ... +85 °C |
| ● during transport | -40 ... +85 °C |
| ● note | 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) |
| **design, dimensions and weights** | |
| design | Media module |
| width | 50 mm |
| height | 22 mm |
| depth | 91 mm |
| net weight | 0.22 kg |
| product feature / conformal coating | No |
| fastening method | screwed |
| ● installation in media module slot | Yes |
| **standards, specifications, approvals** | |
| standard | |
| ● for EMC | FCC Part 15 (Class A), EN55022 (CISPR22 Class A) |
| ● for safety / from CSA and UL | UL 60950-1, CSA C22.2 No. 60950-7 |
| ● for hazardous zone / from CSA and UL | Hazardous Locations: Class 1 Division 2 |
| ● for emitted interference | EN 61000-6-4 (Class A) |
| ● for interference immunity | EN 61000-6-2 |
| laser protection class | 21 CFR Chapter 1, Subchapter J |
| certificate of suitability | EN 61000-6-2, EN 61000-6-10 |


Subject to change without notice
© Copyright Siemens

| | |
|---|---|
| ● 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 | https://support.industry.siemens.com/cs/ww/en/view/109766358 |
| ● to website: Industry Mall/RUGGEDCOM selector | https://www.siemens.com/ruggedcom-selector |
| ● to website: Industrial communication | https://www.siemens.com/simatic-net |
| ● to website: Siemens RUGGEDCOM | https://www.siemens.com/ruggedcom |
| ● to web page: SiePortal | https://sieportal.siemens.com/ |
| ● to website: Image database | https://www.automation.siemens.com/bilddb |
| ● to website: CAx-Download-Manager | https://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 | Miscellaneous | inspection certificate |

**last modified:** 11/14/2025


Subject to change without notice
© Copyright Siemens