

product type designation

RMM2972-2RNA

RUGGEDCOM RMM2972-2RNA, Media Module for RUGGEDCOM RST2228/P, to support HSR/PRP functions, port A and B, 2 x 100/1000 Base-X SFPs (SFPs are not included)



product brand name

RUGGEDCOM

Technical Product Detail Page

<https://l.siemens.com/1P6GK6297-8SB00-2AA0>

suitability for operation

RST2228

interfaces

number of electrical connections

- for network components or terminal equipment / maximum
- for SFP / plug-in

2

2; Supported SFPs: RUGGEDCOM SFP1121-1, SFP1121-1FX2, SFP1131-1FX20, SFP1131-1FX50, SFP1131-1FX90, SFP1122-1SX, SFP1122-1SX2, SFP1132-1LX10, SFP1132-1LX25, SFP1132-1LX40, SFP1132-1LX70, SFP1132-1LX100, SFP1132-1LX115, SFP1132-1BX10R, SFP1132-1BX10T, SFP1132-1BX40R, SFP1132-1BX40T

number of optical interfaces / for network components or terminal equipment / maximum

2

ambient conditions

ambient temperature

- during operation
- during storage
- during transport
- note

-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

IP30 (when installed)

design, dimensions and weights

design

Media module

width

99.4 mm

height

21.6 mm

depth

120.099 mm

product feature / conformal coating

No

fastening method

screwed

- installation in media module slot

Yes

standards, specifications, approvals

standard

- for EMC
- for hazardous zone
- for safety / from CSA and UL

EN55032, IEC/EN 61000-6-2

planned

cCSAus (Compliant with CSA C22.2 No. 60950-1, UL60950-1, EN60950-1, IEC60950-1)

- for hazardous zone / from CSA and UL

planned

- for emitted interference

CISPR32, EN 55032, FCC Part15 Class A, CAN ICES-3 Class A / NMB-3 Class A

• for interference immunity	IEC 61000-6-2
certificate of suitability	
• relating to NEMA	NEMA TS-2 (planned)
• CE marking	Yes
• C-Tick	No
• KC approval	No
• E1 approval	No
• E1 approval	No
• railway application in accordance with EN 50155	No
• railway application in accordance with EN 50121-4	Yes
• railway application in accordance with EN 50124-1	No
• fire protection in accordance with EN 45545-2	No
• IEC 61850-3	Yes
• IEEE 1613	Yes
Marine classification association	
• American Bureau of Shipping Europe Ltd. (ABS)	No
• DNV GL	No

standards, specifications, approvals / Environmental Product Declaration

Environmental Product Declaration	Yes
global warming potential [CO2 eq]	
• total	259.55 kg
• during manufacturing	13.3 kg
• during operation	246.21 kg
• after end of life	0.04 kg

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

other	Environment
-------	-------------

[inspection certificate](#)

[Miscellaneous](#)



last modified:

5/9/2026

