

### product type designation



### RF180C communication module

-- spare part -- RFID communications module RF180C for PROFINET; 2 readers can be connected; without connection block for PROFINET.

### suitability for operation

PROFINET network together with RF200/300/600, MV400/500, MOBY D/E/I/U

### transfer rate

transfer rate / for Industrial Ethernet	10 ... 100 Mbit/s
transfer rate / at the point-to-point connection / serial / maximum	115.2 kbit/s

### interfaces

design of the interface / for point-to-point connection	RS422
number of readers / connectable	2
type of electrical connection	
• of Industrial Ethernet interface	(according to the connection block)
• for supply voltage	(according to the connection block)
design of the interface / to the reader / for communication	M12, 8-pin

### mechanical data

material	Thermoplastic (Valox 467, fiberglass reinforced)
color	IP Basic 714
tightening torque / of the screw for securing the equipment / maximum	3 N·m

### supply voltage, current consumption, power loss

supply voltage / at DC	
• rated value	24 V
•	20 ... 30 V
consumed current	
• at DC / at 24 V / without connected devices / typical	0.1 A
• from supply voltage 1L+ / maximum	1.1 A

### ambient conditions

ambient temperature	
• during operation	0 ... 60 °C
• during storage	-40 ... +70 °C
• during transport	-40 ... +70 °C
protection class IP	IP67
shock resistance	According to IEC 61131-2
shock acceleration	300 m/s²
vibrational acceleration	100 m/s²

### design, dimensions and weights

width	60 mm
height	30 mm
depth	210 mm
net weight	0.21 kg
fastening method	2 x M5 screws
wire length / for RS 422 interface / maximum	1000 m

product features, product functions, product components / general	
display version	4 LEDs per reader connection, 4 LEDs for device status
protocol / is supported / Media Redundancy Protocol (MRP)	No
product function / of the PROFINET IO device / is supported / H-Sync forwarding	No
product function / addressable transponder file handler	Yes
protocol / is supported	
• LLDP	Yes
• PROFINET IO protocol	Yes
• TCP/IP	No
• SNMP v1	Yes
• SNMP v2	No
• SNMP v3	No
• DCP	Yes
• EtherNet/IP protocol	No
• OPC UA	No
product functions / management, configuration, engineering	
type of parameterization	GSDML
type of programming	FB 45, FB 55, ID profile, library with functions
type of computer-switched communication	acyclic communication
standards, specifications, approvals	
certificate of suitability	CE, FCC, cULus, PNO: Conformance Class B
certificate of suitability	
• IECEX	No
MTBF	121 a
accessories	
accessories	Connection block M12 d-coded, 7/8" 5-pin or push-pull
further information / internet links	
internet link	
• to web page: selection aid TIA Selection Tool	<a href="https://www.siemens.com/tstcloud">https://www.siemens.com/tstcloud</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="https://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	
General Product Approval	



[Declaration of Con-  
formity](#)



[Miscellaneous](#)

General Product Ap-  
proval

EMV

Environment



[KC](#)



[Confirmation](#)

---

last modified:

10/29/2024 