# SIEMENS

## Data sheet

### 6GT2002-4JD00



Connection block for RF18xC, M12, 7/8" 4-pin

- - spare part - - RFID Ethernet connection block, M12, 7/8 4-pole for RF182C, RFID181EIP.

suitability for operation	Connection block for RF180C, RF182C, RFID 181EIP				
transfer rate					
transfer rate / for Industrial Ethernet	10 100 Mbit/s				
interfaces					
type of electrical connection					
<ul> <li>of Industrial Ethernet interface</li> </ul>	M12, d-coded				
for supply voltage	7/8" 4-pin				
mechanical data					
material	Die-cast zinc				
color	silver				
tightening torque / of the screw for securing the equipment / maximum	1.3 N·m				
supply voltage, current consumption, power loss					
supply voltage / at DC					
rated value	24 V				
•	20 30 V				
continuous current / for loop-through to further bus nodes / at DC / maximum	8 A				
ambient conditions					
ambient temperature					
during operation	0 60 °C				
<ul> <li>during storage</li> </ul>	-40 +70 °C				
during transport	-40 +70 °C				
protection class IP	IP67				
shock resistance	According to IEC 61131-2				
shock acceleration	300 m/s <sup>2</sup>				
vibrational acceleration	100 m/s <sup>2</sup>				
design, dimensions and weights					
width	60 mm				
height	24 mm				
depth	79 mm				
net weight	0.23 kg				
fastening method	4 screws included				
product features, product functions, product components / general					
display version	4 LEDs for Ethernet status				
standards, specifications, approvals					
certificate of suitability	CE, FCC, cULus				
MTBF	1100 a				
further information / internet links					

#### internet link

- to web page: selection aid TIA Selection Tool
- to website: Image database
- to website: CAx-Download-Manager
- to website: Industry Online Support

#### security information

security information

https://www.siemens.com/tstcloud https://www.automation.siemens.com/bilddb https://www.siemens.com/cax https://support.industry.siemens.com

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					
Declaration of Con- formity EG-Konf.	UK CA		EHC	UL u	
General Product Approval	EMV	Environment			
Miscellaneous RCM	KC	<u>Confirmation</u>			
last modified: 2/18/2025 C					