# **SIEMENS**

#### **Data sheet**

### 6AG1500-0EA02-2AA0

#### product type designation

## **PROFIBUS** connector

SIPLUS NET PB Connector based on 6GK1500-0EA02 with conformal coating, -25...+60  $^{\circ}\text{C},$ 



transfer rate	
transfer rate / with PROFIBUS	9.6 kbit/s 12 Mbit/s
ambient conditions	
ambient temperature	
<ul> <li>in horizontal mounting position / during operation</li> </ul>	7040 °C
<ul> <li>during storage and transport</li> </ul>	7040 °C
relative humidity	
<ul> <li>with condensation / according to IEC 60068-2-38 / maximum</li> </ul>	100 %; RH incl. condensation / frost (no commissioning in bedewed state), horizontal installation
type of coating	
<ul> <li>for electronic devices in railway applications according to EN 50155</li> </ul>	Yes; Class PC2 protective coating acc. to EN 50155:2017
standards, specifications, approvals	
reference code	
<ul> <li>according to IEC 81346-2</li> </ul>	X
<ul> <li>according to IEC 81346-2:2019</li> </ul>	XGA
further information / internet links	
internet link	
• to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
<ul> <li>to web page: selection aid TIA Selection Tool</li> </ul>	https://www.siemens.com/tstcloud
<ul> <li>to website: Industrial communication</li> </ul>	https://www.siemens.com/simatic-net
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

security information

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







**Miscellaneous** 

Manufacturer Declaration

last modified: 12/9/2024 🖸