

### product type designation

product description

### PB BFOC Plug PCF

BFOC screw-connector for PCF-fibre optic cable with plastic Cladding

BFOC plug PCF for on-site assembly to PCF FOC cables pack: 20 units +cleaning cloths.



Figure similar

suitability for use

For connection of PCF fiber-optic cables

### transfer rate

transfer rate / with PROFIBUS

9.6 kbit/s ... 12 Mbit/s

### interfaces

number of optical interfaces / for fiber optic cable

1

design of the optical interface / for network components or terminal equipment

BFOC connector

type of electrical connection / FastConnect

No

### mechanical data

material / of the enclosure

Metal and plastic

locking mechanism design

Bayonet

### design, dimensions and weights

type of cable outlet

180° cable outlet

width

10 mm

height

10 mm

depth

10 mm

net weight

8 g

### ambient conditions

protection class IP

IP20

### product features, product functions, product components / general

product feature

- silicon-free

Yes

product component

- strain relief

Yes

### standards, specifications, approvals

certificate of suitability

- RoHS conformity
- UL approval
- railway application in accordance with EN 50155

Yes

No

No

reference code

- according to IEC 81346-2:2019

XHA

### further information / internet links

internet link

- to website: Selection guide for cables and connectors
- to web page: selection aid TIA Selection Tool
- to website: Industrial communication
- to web page: SiePortal

<https://support.industry.siemens.com/cs/ww/en/view/109766358>

<https://www.siemens.com/tstcloud>

<https://www.siemens.com/simatic-net>

<https://sieportal.siemens.com>

- to website: Image database
- to website: CAx-Download-Manager
- to website: Industry Online Support

<https://www.automation.siemens.com/bilddb>  
<https://www.siemens.com/cax>  
<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](http://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

Environment

[Declaration of Con-  
formity](#)



[Manufacturer Declara-  
tion](#)



[Confirmation](#)

Industrial Communication

[PROFINET](#)

last modified:

12/9/2024 