SIEMENS

Data sheet

6GK7342-5DA03-0XE0

product type designation



CP 342-5

Communications processor CP 342-5 for connection of SIMATIC S7-300 to PROFIBUS DP, S5-compatible, PG/OP and S7 communication.

transfer rate • at the 1st interface / according to PROFIBUS interfaces	9.6 kbit/s 12 Mbit/s
-	9.6 kbit/s 12 Mbit/s
interfaces	
number of interfaces / according to Industrial Ethernet	0
number of electrical connections	
 at the 1st interface / according to PROFIBUS 	1
for power supply	1
type of electrical connection	
 at the 1st interface / according to PROFIBUS 	9-pin Sub-D socket (RS485)
for power supply	4-pole terminal block
supply voltage, current consumption, power loss	
type of voltage / of the supply voltage	DC
supply voltage / 1 / from backplane bus	5 V
supply voltage / external	24 V
supply voltage / external / at DC / rated value	24 V
relative positive tolerance / at DC / at 24 V	20 %
relative negative tolerance / at DC / at 24 V	15 %
consumed current	
from backplane bus / at DC / at 5 V / typical	0.15 A
• from external supply voltage / at DC / at 24 V / typical	0.25 A
power loss [W]	6.75 W
ambient conditions	
ambient temperature	
during operation	0 60 °C
during storage	-40 +70 °C
during transport	-40 +70 °C
relative humidity	
 at 25 °C / without condensation / during operation / maximum 	95 %
protection class IP	IP20
design, dimensions and weights	
module format	Compact module S7-300 single width
width	40 mm
height	125 mm
depth	120 mm
net weight	0.3 kg
product features, product functions, product components / ger	neral
number of units	

16
16
240 byte
V
Yes
124
124
2160 hyta
2160 byte
2160 byte
244 byte
244 byte
240 byte
Vee
Yes
040 h. 4-
240 byte
240 byte
16
32
28
No
STEP 7 V5.1 SP2 or higher / STEP 7 Professional V12 (TIA Portal) or higher
Yes; GB3836.1, GB3836.8
Ex nA IIC T4 Gc
eclaration
Yes
229.03 kg
17.48 kg
211.2 kg
0.35 kg
https://www.automation.siemens.com/bilddb
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

Manufacturer Declaration



Declaration of Conformity







For use in hazardous locations

Marine / Shipping





<u>FM</u>

CCC-Ex





Environment

Confirmation



last modified:

3/22/2024

