SIEMENS

Data sheet 6GK7342-5DF00-0XE0

product type designation	**CP 342-5 FO**
	********** spare part ********* communications processor CP 342-5 FO for connection of SIMATIC S7-300 to PROFIBUS DP, S5-compatible, PG/OP and S7 communication.



product brand name	SIMATIC NET
transfer rate	
transfer rate	
● at the 1st interface / according to PROFIBUS	9.6 kbit/s ... 12 Mbit/s
interfaces	
number of interfaces / according to Industrial Ethernet	0
number of electrical connections	
● for power supply	1
type of electrical connection	
● 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	24 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 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
width	40 mm
height	125 mm
depth	120 mm
net weight	0.3 kg
fastening method	

Subject to change without notice
© Copyright Siemens

● S7-300 rail mounting	Yes
product features, product functions, product components / general	
number of units	
● per CPU / maximum	4
wire length	
● for PCF FOC / maximum	300 m
● for POF FOC / maximum	50 m
performance data / open communication	
number of possible connections / for open communication / by means of SEND/RECEIVE blocks / maximum	16
data volume	
● as user data per connection / for open communication / by means of SEND/RECEIVE blocks / maximum	240 byte
performance data / PROFIBUS DP	
service / as DP master	
● DPV0	Yes
number of DP devices	
● on DP master / operable	124
data volume	
● of the address range of the inputs / as DP master / total	2160 byte
● of the address range of the outputs / as DP master / total	2160 byte
● of the address range of the inputs / per DP device	244 byte
● of the address range of the outputs / per DP device	244 byte
● of the address range of the diagnostic data / per DP device	240 byte
service / as DP device	
● DPV0	Yes
data volume	
● of the address range of the inputs / as DP device / total	240 byte
● of the address range of the outputs / as DP device / total	240 byte
performance data / S7 communication	
number of possible connections / for S7 communication	
● maximum	16
performance data / multi-protocol mode	
number of active connections / with multi-protocol mode	
● without DP / maximum	32
● with DP / maximum	28
performance data / telecontrol	
protocol / is supported	
● TCP/IP	No
product functions / management, configuration, engineering	
configuration software	
● required	STEP 7 V5.1 SP2 or higher / STEP 7 Professional V12 (TIA Portal) or higher
standards, specifications, approvals / hazardous environments / header	
certificate of suitability / CCC / for hazardous zone according to GB standard	Yes
further information / internet links	
internet link	
● to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
● to website: Industrial communication	https://www.siemens.com/simatic-net
● to website: Image database	https://www.automation.siemens.com/bilddb
● to website: CAx-Download-Manager	https://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 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

© Copyright Siemens

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 Conformity | China RoHS | Manufacturer Declaration

General Product Approval | For use in hazardous locations

FM | CCC-Ex

For use in hazardous locations | Maritime application

last modified: 7/16/2026

© Copyright Siemens