SIEMENS

Data sheet 6GK7443-1UX00-0XE0

product type designation	**CP 443-1 OPC UA**



********** spare part ********* communications processor CP 443-1 OPC UA; 1x 10/100/1000 Mbps RJ 45 port; OPC UA communication (data access). operation as OPC UA server operation as OPC UA client via programmable user block according to PLCopen, OPC UA-compliant security mechanisms PG communication time synchronization web diagnostics OPC UA server certification.

product brand name	SIMATIC NET
transfer rate	
transfer rate	
● for Industrial Ethernet	10 ... 1000 Mbit/s
interfaces	
number of interfaces / according to Industrial Ethernet	1
type of electrical connection	
● of Industrial Ethernet interface	RJ45 port
supply voltage, current consumption, power loss	
type of voltage / of the supply voltage	DC
supply voltage / 1 / from backplane bus	5 V
relative symmetrical tolerance / at DC	
● at 5 V	5 %
consumed current	
● from backplane bus / at DC / at 5 V / typical	1.3 A
power loss [W]	6.5 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 S7-400 single width
width	25 mm
height	290 mm
depth	210 mm
net weight	0.7 kg
product features, product functions, product components / general	
number of units	
● per CPU / maximum	1
performance data / S7 communication	
number of possible connections / for S7 communication	
● with PG connections / maximum	2
performance data / as OPC UA server	

Subject to change without notice
© Copyright Siemens

protocol / is supported / OPC UA Server	Yes
number of possible connections / to OPC UA clients / maximum	10
number of variables (items) / maximum	64000
storage capacity / for variables (items) in summary	64000 byte
number of monitorings (subscriptions)	
● per connection / maximum permissible	5
number of variables (items)	
● per monitoring (subscriptions) / maximum	900
storage capacity / for monitored variables (items)	45000 byte
queue size / per monitored variable (item)	2
performance data / as OPC UA client	
protocol / is supported / OPC UA Client	Yes
number of possible connections / for OPC UA server / maximum	5
number of variables (items) / over all connections reading/writing / maximum	10000
product functions / management, configuration, engineering	
protocol / is supported	
● SNMP v1	Yes
● SNMP v3	Yes
configuration software	
● required	STEP 7 V5.5 SP4 HF10 or higher / STEP 7 Professional V14 (TIA Portal) or higher
product functions / diagnostics	
product function / web-based diagnostics	Yes
product functions / security	
product function	
● password protection for Web applications	Yes
● encrypted data transmission	Yes
● switch-off of non-required services	Yes
● log file for unauthorized access	Yes
product functions / time	
protocol / is supported	
● NTP	Yes
● NTP (secure)	Yes
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 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)

© Copyright Siemens

Approvals / Certificates

General Product Approval



Declaration of Conformity





China RoHS

Manufacturer Declaration

General Product Approval





EMV



For use in hazardous locations





FM

For use in hazardous locations

CCC-Ex

Maritime application









NK / Nippon Kaiji Kyokai

Maritime application





CCS (China Classification Society)

last modified: 7/16/2026

Subject to change without notice
© Copyright Siemens