SIEMENS

Data sheet 6GK1562-3AA01

Communications processor CP 5623 A2 PCI Express X1 (3. 3 V) for connection to PROFIBUS; incl. configuration tool and DP-Base software: DP-RAM interface for DP master incl. PG and FDL protocol, single license for 1 installation, runtime software, class A; software and electronic manual on DVD, 2 languages (de, en) ; operating system support see SIMATIC NET software.

transfer rate	
transfer rate	
● at the 1st interface / according to PROFIBUS	9.6 kbit/s ... 12 Mbit/s
interfaces	
number of electrical connections	
● at the 1st interface / according to PROFIBUS	1
type of electrical connection	
● at the 1st interface / according to PROFIBUS	9-pin Sub-D socket (RS 485)
● of the backplane bus	PCI Express x1
supply voltage, current consumption, power loss	
type of voltage / of the supply voltage	DC
supply voltage	
● 1 / from backplane bus	3.3 V
● 2 / from backplane bus	12 V
relative symmetrical tolerance / at DC	
● at 3.3 V	9 %
● at 12 V	8 %
consumed current	
● 1 / from backplane bus / at DC / maximum	0.3 A
● 2 / from backplane bus / at DC / maximum	0.25 A
power loss [W]	4 W
ambient conditions	
ambient temperature	
● during operation	5 ... 55 °C
● during storage	-20 ... +60 °C
● during transport	-20 ... +60 °C
relative humidity / at 25 °C / without condensation / during operation / maximum	85 %
protection class IP	IP00
design, dimensions and weights	
module format	PCI Express x1 (half length)
width	18 mm
height	112 mm
depth	101 mm
net weight	0.088 kg
product features, product functions, product components / general	
number of plug-in cards of same design / plug-in / per PC station	4
number of units / note	-
performance data / open communication	

software / for open communication / by means of SEND/RECEIVE / required	FDL driver included in scope of delivery of the CP
number of possible connections / for open communication / by means of SEND/RECEIVE / maximum	80
performance data / PROFIBUS DP	
software / for DP master function / required	No
service / as DP master	
● DPV0	Yes
● DPV1	Yes
● DPV2	Yes
number of DP slaves / on DP master / operable	124
data volume	
● of the address range of the inputs / as DP master / total	30256 byte
● of the address range of the outputs / as DP master / total	30256 byte
● of the address range of the inputs / per DP slave	244 byte
● of the address range of the outputs / per DP slave	244 byte
● of the address range of the diagnostic data / per DP slave	244 byte
software / for DP slave function / required	No
service / as DP slave	
● DPV0	Yes
● DPV1	Yes
data volume	
● of the address range of the inputs / as DP slave / total	244 byte
● of the address range of the outputs / as DP slave / total	244 byte
performance data / S7 communication	
software / for S7 communication / required	yes, HARDNET-PB S7
number of possible connections / for S7/PG communication / maximum	50
performance data / multi-protocol mode	
number of active connections / with multi-protocol mode	50
number of configurable connections / per PC station	207
product functions / management, configuration, engineering	
configuration software / required	Included in scope of supply
product functions / diagnostics	
product function	
● port diagnostics	Yes
standards, specifications, approvals	
reference code	
● according to IEC 81346-2:2019	KEC
further information / internet links	
internet link	
● to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
● to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
● to website: Industrial communication	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 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	Environment

last modified: 7/15/2025