SIEMENS

Data sheet

6GK7243-1EX01-0XE0

product type designation



CP 243-1

******** spare part ******* communications processor CP 243-1 for connection of SIMATIC S7-22X to Industrial Ethernet; FTP client communication; HTTP server; FTP server; Email client.

10 100 Mbit/s
1
1
1
RJ45 port
3-pole terminal block
DC
5 V
24 V
24 V
20 %
15 %
0.06 A
0.053 A
0.06 A
1.5 W
0 45 °C
0 55 °C
-40 +70 °C
-40 +70 °C
95 %
IP20
Compact module S7-200 double width
71.2 mm
71.2 mm 80 mm

number of possible connections / maximum • with PGOP connections / maximum • as a chair / by means of FTP / maximum • as server / by means of FTP / maximum • as server / by means of HTTP / maximum • by server of server / by means of HTTP / maximum • by server of server / by serve		
united of units per CPU / maximum 1	net weight	0.15 kg
profession of the Vision Visi	product features, product functions, product components / gene	eral
number of possible connections / for \$7 communication maximum 8 with PG connections / maximum 1 with PG connections / maximum 8 with PG connections / maximum 8 with PG connections / maximum 8 with PG connections / maximum 1 with PG connections / maximum 8 with PG connections / maximum 1 mumber of possible connections as as client / by means of FTP / maximum 1 number of possible connections as server / by means of FTP / maximum 1 number of possible connections 1 as earned interfer / maximum 1 number of enalls with 1024 characters / of email client / maximum 1 number of access authorizations / of access protection 8 storage capacity / of the user memory a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory 4 a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory 4 a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory 4 a fash memory file system 1 number of access authorizations / of access protection 8 storage capacity / of the user memory 4 a fash memory file system 1 number of access authorization, yes planting 1 yes 2 configuration software 4 required 5 required 5 storage capacity / of the success for access fo	number of units	
performance data (\$7 communication 8	• per CPU / maximum	1
number of possible connections / maximum • with PGOP connections / maximum • as a chair / by means of FTP / maximum • as server / by means of FTP / maximum • as server / by means of HTTP / maximum • by server of server / by means of HTTP / maximum • by server of server / by serve	• note	-
* with PGC connections / maximum * as client / by means of FTP / maximum * as server / by means of FTP / maximum * as server / by means of HTTP / maximum * as server /	performance data / S7 communication	
with PG connections / maximum with PG connections / maximum s with PG connections / maximum s as client / functions number of possible connections	number of possible connections / for S7 communication	
with PGIOP connections / maximum profromations data / Tif functions as a client / by means of FTP / maximum as a server / by means of FTP / maximum as a server / by means of HTTP / m	• maximum	8
number of possible connectors • as selent / by means of FTP / maximum 1 number of possible with 1024 characters / of email client / maximum 1 number of emails with 1024 characters / of email client / maximum 1 number of of emails with 1024 characters / of email client / maximum 1 number of of emails with 1024 characters / of email client / maximum 1 number of occess authorizations / of access protection 8 Milbyte 100000 8 Milbyte 100000 8 Milbyte 100000 9 Fordout file user memory • as flash memory (file system 100000 9 Fordout file system 100000 9 Fordout file system 100000 9 Fordout file file system 100000 9 Fordout file file system 100000 No 100000 9 Fordout file file system No No Configuration s / management. Configuration, engineering product functions / management. Configuration, engineering product file file system No No Configuration software • required STEP 7-Micro/WIN Version V4.0 SP8 or higher Fordout file file file system No Outside file file file file file system No No Configuration software • required STEP 7-Micro/WIN Version V4.0 SP8 or higher Fordout functions / visition No Outside file file file file file file file fil	 with PG connections / maximum 	1
number of possible connections a as client / by means of FTP / maximum 1	 with PG/OP connections / maximum 	8
as aclient / by means of FTP / maximum as server / by means of HTP / maximum as server / by means of HTP / maximum as semal client / maximum as flash memory file system as flash memory file system amber of possible centre of the flash memory cells broformance distal / telecontrol protocol / is supported	performance data / IT functions	
number of possible connections * as server! by means of HTTP / maximum * as server! by means of HTTP / maximum 1 number of emails with 1024 characters / of email client / maximum number of emails with 1024 characters / of email client / maximum number of access authorizations / of access protection 8 torage capacity / of the user memory * as flash memory file system number of possible write cycles / of the flash memory cells protocol / is supported * 1 CP/IIP protocol / is supported * 1 CP/IIP reduct function / MIB support protocol / is supported * 1 CP/IIP * SNRP Y	number of possible connections	
	as client / by means of FTP / maximum	1
	number of possible connections	
	as server / by means of HTTP / maximum	4
maximum umber of access authorizations / of access protection storage capacity / of the user memory • as flash memory file system umber of possible write cycles / of the flash memory cells performance data / telecontrol protocol / is supported • TCP/IP roduct function / MIB support • SIME y1 configuration software • (RME y1 configuration software • (acquired • Product function / web-based diagnostics roduct function / web-based diagnostics roduct function / internet links internet link • (a web page: selection aid TIA Selection Tool • (b web page: selection aid TIA Selection Tool • (b website: Image database • (b website: Image database • (b website: Image database • (b website: Image transport of the support of this //survey siemens.com/simalic-net bitto: //survey siemens.com/cax • (b website: Industry of lines Support • (b website: Industry of lines Support) • (b website: Industry of lines S	-	1
storage capacity / of the user memory • as flash memory file system a flowood performance data / telecontrol protocol / is supported • TCPIP reduct functions / management, configuration, engineering product function / MIB support • SNMP v1 No configuration software • required • required • required • required • STEP 7-MicroWIN Version V4.0 SP8 or higher reduct function / web-based diagnostics product function / web-based diagnosti		32
storage capacity / of the user memory • as flash memory file system Inumber of possible write cycles / of the flash memory cells operformance data / telecontrol protocol / is supported • TCPIP Yes oroduct functions / management, configuration, engineering product function / MIB support • SNMP v1 No configuration software • required • SNMP v1 No configuration software • required soroduct functions / diagnostics product functions / switch product function / web-based diagnostics No No Internet link internet l	number of access authorizations / of access protection	8
* as flash memory file system * number of possible write cycles / of the flash memory cells * 100000 protocol / is supported * TCPIPP * Yes product functions / management, configuration, engineering product function / MiB support * SNMP v1 * No * SNMP v1 * No * SNMP v1 * SNMP v1 * SNMP v1 * Supported * Fequired * Fequired * STEP 7-Micro/WIN Version V4.0 SP8 or higher product function / web-based diagnostics product function / web-based diagnostics product function / switch product fasture / switch * No **To web page: selection aid TIA Selection Tool **Io web page: selection aid TIA Selection Tool **Io website: Industrial communication **Io website: CAx-Download-Manager **Io website: CAx-Download-Manager **Io website: Industry Online Support **Into/Mutmation siemens.com/biddb **Intos/Noww.siemens.com/simatic-net **Int	·	
number of possible write cycles / of the flash memory cells performance data / telecontrol protocol / is supported • TCP/IP Yes Product functions / management, configuration, engineering product function / MIB support • SNMP V1 No configuration software • required • STEP 7-Micro/WIN Version V4.0 SP8 or higher product function / web-based diagnostics product function / web-based diagnostics product function / web-based diagnostics product function / switch product function / internet links • to web page: selection aid TIA Selection Tool • to website: industrial communication • to website: industrial communication • to website: inage database • to website: CAx-Download-Manager • to website: industrial communication security information Security information Security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, against cyber threats, it is necessary to implement—and continuously maritain — a holistic, state—of-the—art industrial cybersecurity functions networks against cyber threats, it is necessary to implement—and continuously maritain — a holistic preventing unauthorized access to their plants, systems, machines and on enteryors and only when appropriate security encounted to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connected to an enterprise network or the intense should only be connect		8 Mibyte
protocol / is supported	·	
TCP/IP Yes TCP/IP Yes No No SMMP v1 No configuration software • required • STEP 7-Micro/WIN Version V4.0 SP8 or higher product function / web-based diagnostics No		
TCP/IP Yes TCP/IP Yes No No SMMP v1 No configuration software • required • STEP 7-Micro/WIN Version V4.0 SP8 or higher product function / web-based diagnostics No	protocol / is supported	
product function / MIB support		Yes
product function / MIB support	product functions / management, configuration, engineering	
protocol / is supported SNMP v1 No configuration software required sreduct functions / diagnostics product function / web-based diagnostics product function / web-based diagnostics required solve function / web-based diagnostics required solve function / web-based diagnostics required solve function / switch required solve function / switch required solve function / switch required solve function / witch required solve function / diagnostics Yes required solve function / witch solve function / witch to web selection aid TIA Selection Tool https://www.siemens.com/istaloud ht		No
SIMP V1 configuration software required required STEP 7-Micro/WIN Version V4.0 SP8 or higher reduct functions / diagnostics product functions / switch product functions / switch product function / web-based diagnostics reduct feature / switch No further information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industrial communication • to website: CAx-Download-Manager • to website: Industry Online Support https://www.siemens.com/simatic-net https://www.siemens.com/simatic-net https://www.siemens.com/cax • to website: Industry Online Support https://swup.siemens.com/cax security information security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of 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 that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that place. For additional information on industrial cybersecurity measures 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. (v4.7.7)	·	
required STEP 7-Micro/WIN Version V4.0 SP8 or higher product functions / diagnostics product function / web-based diagnostics Yes product functions / switch product feature / switch No further information / internet links internet link • to web page: selection aid TIA Selection Tool https://www.siemens.com/istcloud • to website: Industrial communication https://www.siemens.com/simatic-net https://www.siemens.com/simatic-		No
required STEP 7-Micro/WIN Version V4.0 SP8 or higher product functions / diagnostics product function / web-based diagnostics Yes product functions / switch product feature / switch No further information / internet links internet link • to web page: selection aid TIA Selection Tool https://www.siemens.com/istcloud • to website: Industrial communication https://www.siemens.com/simatic-net https://www.siemens.com/simatic-	configuration software	
product function / web-based diagnostics product functions / switch product feature / switch product feature / switch No further information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: Image database • to website: Industry Online Support Security information Security information	-	STEP 7-Micro/WIN Version V4.0 SP8 or higher
product function / web-based diagnostics product functions / switch product feature / switch product feature / switch No further information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: Image database • to website: Industry Online Support Security information Security information	product functions / diagnostics	
product feature / switch further information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support **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 are applied as soon as they are available and that the latest 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)	product function / web-based diagnostics	Yes
Internet link Intern	product functions / switch	
internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industry Online Support • to website: Industry Online Support 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. 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 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)	product feature / switch	No
to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Image database to website: CAx-Download-Manager to website: Industry Online Support to website: Industry Online Support 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 a 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 a 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 a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/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 u	further information / internet links	
to website: Industrial communication to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://www.siemens.com/cax to website: Industry Online Support 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)	internet link	
to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://support.industry.siemens.com/ security information 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-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/cett. (V4.7)		
to website: CAx-Download-Manager to website: Industry Online Support 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)	 to web page: selection aid TIA Selection Tool 	https://www.siemens.com/tstcloud
to website: CAx-Download-Manager to website: Industry Online Support 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)	. 3	
• to website: Industry Online Support https://support.industry.siemens.com 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)	to website: Industrial communication	https://www.siemens.com/simatic-net
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)	 to website: Industrial communication to website: Image database	https://www.siemens.com/simatic-net http://automation.siemens.com/bilddb
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)	 to website: Industrial communication to website: Image database to website: CAx-Download-Manager 	https://www.siemens.com/simatic-net http://automation.siemens.com/bilddb https://www.siemens.com/cax
· · · · · · · · · · · · · · · · · · ·	 to website: Industrial communication to website: Image database to website: CAx-Download-Manager 	https://www.siemens.com/simatic-net http://automation.siemens.com/bilddb https://www.siemens.com/cax
Approvals / Certificates	to website: Industrial communication to website: Image database to website: CAx-Download-Manager to website: Industry Online Support security information	https://www.siemens.com/simatic-net http://automation.siemens.com/bilddb https://www.siemens.com/cax 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



Declaration of Conformity









EMV For use in hazardous locations

Marine / Shipping

<u>KC</u>



€x

<u>FM</u>

CCC-Ex



Marine / Shipping

Environment







Confirmation

last modified:

8/9/2024

