SIEMENS

Data sheet

6GK7343-1EX30-0XE0

product type designation



CP 343-1

Communications processor CP 343-1 for connection of SIMATIC S7-300 to Industrial Ethernet via ISO and TCP/IP, PROFINET IO controller or PROFINET IO device, integrated 2-port switch ERTEC 200, S7 communication, fetch/write, SEND/RECEIVE RFC1006, multicast, DHCP, NTC- CPU sync, with and without diagnostics, initialization via LAN, 2x RJ45 connection for LAN with 10/100 Mbit/s.

transfer rate			
transfer rate			
 at the 1st interface 	10 100 Mbit/s		
interfaces			
number of interfaces / according to Industrial Ethernet	2		
number of electrical connections			
 at the 1st interface / according to Industrial Ethernet 	2		
for power supply	1		
type of electrical connection			
 of Industrial Ethernet interface 	RJ45 port		
 at the 1st interface / according to Industrial Ethernet 	RJ45 port		
type of electrical connection			
 for power supply 	2-pole plugable 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 	0.2 A		
 from external supply voltage / at DC / at 24 V / typical 	0.16 A		
 from external supply voltage / at DC / at 24 V / maximum 	0.2 A		
power loss [W]	5.8 W		
ambient conditions			
ambient temperature			
 for vertical installation / during operation 	0 40 °C		
 for horizontally arranged busbars / 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	0.22 kg
fastening method	
S7-300 rail mounting	Yes
performance data / open communication	
number of possible connections / for open communication / by	16
means of SEND/RECEIVE blocks / maximum	
data volume	
 as user data per ISO connection / for open communication / by means of SEND/RECEIVE blocks / maximum 	8 Kibyte
 as user data per ISO on TCP connection / for open communication / by means of SEND/RECEIVE blocks / maximum 	8 Kibyte
 as user data per TCP connection / for open communication / by means of SEND/RECEIVE blocks / maximum 	8 Kibyte
 as user data per UDP connection / for open IE communication / by means of SEND/RECEIVE blocks / maximum 	2 Kibyte
number of Multicast stations	16
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	32
performance data / PROFINET communication / as PN IO control	ller
number of PN IO devices / on PROFINET IO controller / operable / total	32
number of external PN IO lines / with PROFINET / per rack	1
data volume	
 as user data for input variables / as PROFINET IO controller / maximum 	1 Kibyte
 as user data for output variables / as PROFINET IO controller / maximum 	1 Kibyte
 as user data for input variables per PN IO device / as PROFINET IO controller / maximum 	1433 byte
 as user data for output variables per PN IO device / as PROFINET IO controller / maximum 	1433 byte
 as user data for input variables per PN IO device / for each sub-module as PROFINET IO controller / maximum 	240 byte
 as user data for output variables per PN IO device / for each sub-module as PROFINET IO controller / maximum 	240 byte
performance data / PROFINET communication / as PN IO device	
product function / PROFINET IO device	Yes
data volume	
 as user data for input variables / as PROFINET IO device / maximum 	512 byte
 as user data for output variables / as PROFINET IO device / maximum 	512 byte
 as user data for input variables / for each sub-module as PROFINET IO device 	240 byte
 as user data for output variables / for each sub-module as PROFINET IO device 	240 byte
 as user data for the consistency area for each sub- module 	240 byte
number of submodules / per PROFINET IO-Device	32
performance data / telecontrol	
protocol / is supported	
• TCP/IP	Yes
product functions / management, configuration, engineering	
product function / MIB support	Yes
protocol / is supported	
• SNMP v1	Yes
• DCP	Yes
• LLDP	Yes

identification & maintenance function (identification & maintenance function) (identification & maintenance function) (identification & identification designation) (identification & identification designation) (identification & identification &		
identification & maintenance function i & MAD - elow-specific information i & MAD - elow-specific information i & MAD - elow-specific information i & MAD - e	configuration software	
• MAD• Yes• BAD• Select spacetic informationYesproduct functions / disputationYesproduct functions / disputationYes• with HT / PROFINET IO softYes• with GP / GP	required	STEP 7 V5.4 SP2 or higher / STEP 7 Professional V11 (TIA Portal) or higher
• Wa Yes product functions / leagnostics. Yes product function / web based disposts Yes product function / web applications Yes product function / web applications No • with/-managad No • with/-managad Yes • with/-managad No • with/-managad Yes • with/-managad Yes • with/-managad No • with/-managad Yes • with/-managad No • origination with STEP ? Yes product function Yes • origination with STEP ? Yes product function Yes • origination with STEP ? No product functions / security No product functions / security No • originations / security No	identification & maintenance function	
product function / desponsition product function / such product function / such product function outlet function / such product function outlet function outlet function outlet o	 I&M0 - device-specific information 	Yes
product function / web-based diagnosities Yes product functions / switch product function / switch entition-managed entit Inctions / switch interdinations / switch entition with IRT / PROFINET IC switch entition / SUCCOM Support IC IC 1945 & 2019 Intervalues atomatics of IRT / Intervalues IC	 I&M1 - higher level designation/location designation 	Yes
product functions / switch Yes • witch managed No • with RT RPORTNET to switch Yes • ondputation with STE P Yes product function * • end reading managed No • readuct function * • end reading managed No • readuct functions / security Yes product function * • experiment function * • ACL - IP-based Yes • ACL - IP-based for PLCPould reavices Yes • Order function of pass on the synchronization Yes • Reading of communication via physical ports Yes • No Yes product function of Just portrol data charactions approvals Yes product function of Just portrol data charactions approvals Yes product function of Just portrol data charactions approvals Yes reference code * No • weebrige: industrial communication Ithttp:/	product functions / diagnostics	
product feature / avetch Yes product function • • with-invariaged No • • No • onofiguation with STEP 7 Yes product functions redundancy yes product functions / redundancy Yes No • • ing redundancy Yes • • No Popolation / supported //	product function / web-based diagnostics	Yes
product function	product functions / switch	
switch-managed No witch-managed No witch-managed ves/product functions redundancy roduct function ining redundancy redundancy redundancy roduct function ining redundancy ining inining ining inininining inin	product feature / switch	Yes
• switch managed No • witch IRT / ROFINET IO switch Yes • ondiguation with STEP 7 Yes product function • • ring redundancy Yes • edundancy manager No • edundancy second protection for Web applications No • elassword protection for Web applications No • elassword protection in group of the second	product function	
• with IRT / PROFINET IO switch Yes • ondiguration with STEP 7 Yes product function / relundancy Yes product function / supported / Media Redundancy Protocol (MRP) Yes product function / security Yes • CAL : IP-Deased Yes • CAL : IP-Deased / Security Yes • Security of on-required services Yes • Big file for unsubtractal access No • Security of the for unsubtractal access Yes • NTP Yes • NTP Yes • Second that function / Step 22019 KEC • Web page: selection and TAS election Tool https://www.siemens.com/tabland • Web page: selection and TAS election Tool https://www.siemens.com/tabland • Web page: selection and TAS election Tool https://www.siemens.com/tabland		No
• onfgration with STEP 7 Yes voduct functions / redundancy Yes • ing redundancy Yes • ing redundancy Yes • indigration with STEP 7 Yes • absolut for for the applications Yes • absolut for for non-trading to indigration of the applications Yes • blocking of communication on uphysical ports Yes • product function / StCLOCK support Yes • product function / Stand provids Yes • other of the application of a support of approvals Yes • other of the application of the application of the application of the application of application of approvals Yes • other of the application t	5	
product function engredundancy edundancy manager No edundancy manager No protoct / is supported / Media Redundancy Protocol (MRP) Yes reserveduct functions / security product functions / security manager expression of the security No product functions / regular security No product functions / regular security No product functions / regular security No rederence		
product function		
ining redundancy indundancy manager No indundancy manager indundancy Protocol (MRP) indundancy Protocol (MRP) indundancy Protocol (MRP) indundancy Protocol (MRP) indundancy indundancy Protocol (MRP) indundancy indundancy Protocol (MRP) indundancy in		
nedundarcy manager No protocol /s supported / Media Redundancy Protocol (MRP) Yes product function No • assawrd protection for Web applications No • ACL - IP-Deased Yes • ACL - IP-Deased Yes • action-required services Yes • blocking of communication via physical ports Yes • blocking of communication via physical ports Yes • product function / SICLOCK support Yes reference code - • according to IEC 81346-2:2019 KEC uther Information / Internet link - • to web page: selection aid TIA Selection Tool https://www.silemens.com/sitale.ud • to web page: selection aid TIA Selection Tool https://www.silemens.com/sitale.ud • to web page: selection aid TIA Selection Tool https://www.silemens.com/sitale.ud • to websits		Ves
protocol / is supported / Media Redundancy Protocol (MRP) product functions / security product function		
product function No • password protection for Web applications No • ACL - IP-based Yes • ACL - IP-based of PLC/routing No • witch-off of non-require services Yes • blocking of communication via physical ports Yes • blocking of communication via physical ports Yes • ordict functions / Istice No product function / SICLOCK support Yes product function / SICLOCK support Yes product functions / specifications, approvals Yes reference code - • according to IEC 81346-2:2019 KEC urther information / Internet links Inters://www.siemens.com/Isiloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/Isiloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/Isiloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/Isiloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/Isiloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/Isiloud • to website: Industrial communication https://www.sie	· · · · · · · · · · · · · · · · · · ·	
product function	· · · ·	165
password protection for Web applications No ACL - IP-based Yes ACL - IP-based for PLC/routing No switch-off of non-required services Yes blocking of communication via physical ports blocking of communication product function / SICLOCK support ves product function / SICLOCK support ves product function / SICLOCK support ves product function / Intervet Intex ference code according to IEC 81346-2:2019 KEC urther information / Intervet Intex interret link lo web page: selection aid TIA Selection Tool bu website: Industrial communication bu web page: selection aid TIA Selection Tool bu website: Industrial communication bu website: Industrial communication bu website: Industrial communication bu website: Industrial comport bu website: Industrial communication bu website: Industrial communication bu website: Industrial coherecomport bu website: Industrial coherecomportine secure phy		
 ACL - IP-based Yes ACL - IP-based for PLC/routing No switch-off on required services Yes blocking of communication via physical ports Yes product function / IsCLOCK support Yes product function / IsCLOCK support Yes protocul / is supported NTP Yes cacording to IEC 81346-2:2019 KEC uther information / Internet links internet link internet link internet link internet link internet link interview sitemens com/tstoloud thus //www silemens com/tstoloud thus //www silemens		Ne
• ACL - IP-based for PLC/routing No • witch-off of non-required services Yes • blocking of communication via physical ports Yes • log file for unauthorized access No product functions / time ************************************		
 switch-off of non-required services blocking of communication via physical ports No Yes log file for unauthorized access No product function / SICLOCK support Yes product function / SICLOCK support Yes product function / SICLOCK support Yes protocol / is supported NTP Yes reference code according to IEC 81346-2:2019 KEC urther information / internet links internet link to web page: selection aid TIA Selection Tool https://sigportal.siemens.com/Stoloud to website: Industrial communication https://www.siemens.com/Stoloud to website: Industrial communication https://www.siemens.com/Last to website: Industrial cybersecurity function https://sigport.industry.siemens.com/Last to website: Industrial cybersecurity function https://sigport.industry.siemens.com/Last security information 		
• blocking of communication via physical ports Yes • log file for unauthorized access No oroduct functions / time product function / SICLOCK support Yes product function / pass on time synchronization Yes product function, supported * • NTP Yes • NTP Yes • cacording to IEC 81346-2:2019 KEC • uther information / Internet link Interview signmens.com/stoloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/stoloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/stoloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/stoloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/stoloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/stoloud • to web site: CAx-Download-Manager https://www.siemens.com/stoloud • to website: Industry Online Support https://www.siemens.com/stolous security information Seiemes provides products and solutions with industrial cybersecurity function and the state-of-the-ait industrial cybersecurity oncept. Siemens and networks against cyber security information Seiemens provides products and solutions w	-	
• log file for unauthorized access No product function / time	•	
product function / IsiCLOCK support Yes product function / Jass on time synchronization Yes protocol / is supported		
product function / SICLOCK support Yes product function / pass on time synchronization Yes protocol / is supported Yes NTP Yes tandards, specifications, approvals reference code • according to IEC 81346-2:2019 KEC uther information / Internet links internet link • to web page: selection aid TIA Selection Tool https://www.siemens.com//simdic-net • to web page: Selection aid TIA Selection Tool https://www.siemens.com//simdic-net • to website: Industrial communication https://www.siemens.com/ • to website: Industrial control https://www.siemens.com//simdic-net https://www.siemens.com/ https://www.siemens.com/ • to website: Industrial control https://www.siemens.com/ • to website: Industrial control https://www.siemens.com/ • to website: Industry Online Support https://www.siemens.com/ • to website: Industry Online Support https://www.siemens.com/ • security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function for prevent		No
product function / pass on time synchronization Yes protocol / is supported	product functions / time	
protocol / is supported Yes standards, specifications, approvals reference code according to IEC 81346-2:2019 KEC urther information / internet links internet link internet link https://www.siemens.com/tstcloud it o web page: selection aid TIA Selection Tool https://www.siemens.com/statcloud it o web page: SiePortal https://www.siemens.com/ it o website: Industrial communication https://www.siemens.com/bilddb it o website: CAx-Download-Manager https://www.siemens.com/cax it o website: Industry Online Support https://www.siemens.com/bilddb security information Siemens provides products and solutions with industrial cybersecurity functic that support the secure operation of plants, systems, machines and networks in order to protect plants, systems, machines and networks in order to protect plants, systems, machines and networks on order to protect plants, systems, machines and networks in order to protect plants, systems, machines and networks against cyber if or preventing unauthorized access to their plants, systems, machines and networks against cyber firewalts and/or preventing unauthorized access to their plants, systems, machines and networks against cyber security information Siemens ond/or the internet if and to the extent such a connection networks sign of such and solutions constitute one element of such a concel. Customers are responsif or preventing unauthorized access to their p	product function / SICLOCK support	Yes
NTP Yes tandards, specifications, approvals reference code according to IEC 81346-2:2019 KEC utther information / internet links to web page: selection aid TIA Selection Tool https://www.siemens.com/tstcloud to website: industrial communication https://seportal.siemens.com/simatic-net to website: industrial communication https://seportal.siemens.com/bilddb https://seportal.siemens.com/bilddb to website: Industrial communication https://support.industry.siemens.com/bilddb to website: industry Online Support https://support.industry.siemens.com/bilddb to website: industry Online Support to website: industry Online Support security information Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and networks in order to protect plants, systems, machines and networks in order to protect plants, systems, machines and networks solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks us of systems, machines and one-tworks against cyber thevorks.Such systems, machines and one-tworks against cyber thereats, it is necessary to implement – and continuously maintian – a holistic state-of-the-art industrial cybersecurity concept. Siemens is products and solutions on industrial cybersecurity measures (e.g. freevalls and/ networks.Such systems, machines and networks against cyber inevorks.Such systems, machines and one-tworks against cyber inderworks.Such systems, machines and one-tworks against cyber eventing unauthorized access to their plants, systems, machines and networks.Such systems, machines and one-tworks against cybersecurity measures (e.g. freevalls and/ networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. freevalls and/ cyberse	product function / pass on time synchronization	Yes
standards, specifications, approvals reference code according to IEC 81346-2:2019 KEC urther information / internet links internet link to web page: selection aid TIA Selection Tool https://www.siemens.com/lsticloud https://www.siemens.com/simatic-net https://www.siemens.com/simatic-net https://www.siemens.com/simatic-net https://www.automation.siemens.com/ldtdb https://www.automation.siemens.com/ldtdb https://www.siemens.com/cax to website: Industry Online Support https://www.siemens.com/aid security information Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and networks. Such systems, machines and networks squarts cyber threats, it is necessary to implement – and continuously maintain – a holistic state-off-he-art industrial cybersecurity medures are responsil for preventing unauthorized access to their plants, systems, machines and networks such systems, machines and networks used solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks such systems, machines and netw	protocol / is supported	
reference code according to IEC 81346-2:2019 KEC Internet link to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: Image database to website: Image database to website: Industry online Support to support on the secure operation of plants, systems, machines and networks scurity information Security induction security information security infor	• NTP	Yes
• according to IEC 81346-2:2019 KEC urther information / internet links internet link • to web page: selection aid TIA Selection Tool https://www.siemens.com//tsticloud • to website: Industrial communication https://www.siemens.com//simatic-net • to website: Industrial communication https://www.siemens.com//simatic-net • to website: Industrial communication https://www.siemens.com/ • to website: Industry Online Support https://www.siemens.com/cax • to website: Industry Online Support https://support.industry.siemens.com security information Siemens provides products and solutions with industrial cybersecurity functic 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-ari industrial cybersecurity concept. Clustomers are responsil for preventing unauthorized access to their plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic and only be connect to a enterprise network or the internet if and to the extent such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks such as subtring order to are plant any be implemented, please visit www.siemens.com/bet escurity measures it.a uscore.For additional information on industrial cybersecurity concept. Sustems, machines and networks against cyber recomprise network or the internet if and to the extent such a connector necessary and only when appropriate security measures ith	standards, specifications, approvals	
Curther information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web page: SlePortal • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • to protect plants, systems, machines and networks security information Security information Security information Security information are responsite to protect plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsitor to protect plants, systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connect to an enterprise network or the internet if and to the extent such a connect to an enterprise network or the internet if and to the extent such a connect to an enterprise network segmentation are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, place visit www.siemens.com/segmentation are in place. For additional information on industrial cybersecurity measures that product versions are esponsite and components should only be connect to an enterprise network or the internet if and to the extent such a connect to an enterprise network or the internet i f and to the extent suc	reference code	
internet link https://www.siemens.com/istcloud • to web page: selection aid TIA Selection Tool https://www.siemens.com/istcloud • to website: Industrial communication https://www.siemens.com/simatic-net • to website: Image database https://www.siemens.com/cax • to website: CAx-Download-Manager https://www.siemens.com/cax • to website: Industry Online Support https://support.industry.siemens.com security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and networks In order to protect plants, systems, machines and networks In order to protect plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks Such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks segmentation are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c network segmentation are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www siemens.com/cybersecurity measures that product versions are used. Use of product versions that are comproprise security measures that product versions are applied as soon as they are available and that the latest product versions rear applied as soon as they are available and that the latest product versions rea used. Use of p	 according to IEC 81346-2:2019 	KEC
• to web page: selection aid TIA Selection Toolhttps://www.siemens.com/tstcloud• to website: Industrial communicationhttps://www.siemens.com/simatic-net• to web page: SiePortalhttps://sieportal.siemens.com/• to website: Image databasehttps://www.automation.siemens.com/bilddb• to website: CAx-Download-Managerhttps://www.siemens.com/cax• to website: Industry Online Supporthttps://www.siemens.com/cax• to website: Industry Online Supporthttps://support.industry.siemens.comsecurity informationSiemens provides products and solutions with industrial cybersecurity functionsecurity informationSiemens provides products and solutions with industrial cybersecurity functionsecurity informationSiemens provides products and solutions with industrial cybersecurity function an enterprise network or the internet if and to the extent such a concept. Customers are responsite for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks. Such systems, machines and components should only be connect necessary and only when appropriate security measures (e.g. firewalls and/on networks. Such systems, machines and components should only be connect necessary and only when appropriate security measures (e.g. firewalls and/on networks. Such systems, machines and components should only be connect necessary and only when appropriate security measures (e.g. firewalls and/on networks segmentation) are in place. For additional information on industrial cybersecurity notacets and solutions undergo continuous development to make them more secure. Siemens's products and solutions undergo continuous development to apply the latest updates may increase customer's htay fouct versions that an to longer supported, and failure to app	urther information / internet links	
• 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 Siemens provides products and solutions with industrial cybersecurity functic state-of-the-art industrial cybersecurity functic state-of-the-art industrial cybersecurity functic state-of-the-art industrial cybersecurity machines and networks in order to protect plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems machines and networks. Such systems, machines and onetworks. Such systems, machines and onetworks 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. Siemens' product san dolutions undergo continuous development to make them more secure. Siemens strout recomments that product versions are used. Use of product versions that and on the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens' noduct updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens' noduct updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens' noduct ve	internet link	
 to web page: SiePortal https://sieportal.siemens.com/ to website: Image database to website: CAx-Download-Manager thttps://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 function the secure operation of plants, systems, machines and networks in order to protect plants, systems, machines and networks in order to protect plants, systems, machines and networks solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks such systems, machines and on industrial cybersecurity measures (e.g. firewalls and/c network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/c networks segmentation are used. Use of product versions that an to latest product versions are used. Use of product versio	 to web page: selection aid TIA Selection Tool 	https://www.siemens.com/tstcloud
• 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 Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and onecord necessary and only when appropriate security measures (e.g. firewalls and/c network segmentation) are in place. For additional information on industrial cybersecurity measures (c.g. firewalls and/c network segmentation) are in place. For additional information on undergo continuous development to make them more secure. Siemens store recommends that product updates are applied as soon as they are available and hat the latest product versions are used. Use of product versions that an to longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens. Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert	 to website: Industrial communication 	https://www.siemens.com/simatic-net
• to website: CAx-Download-Manager https://www.siemens.com/cax • to website: Industry Online Support https://support.industry.siemens.com security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity function security information Siemens provides products and solutions with industrial cybersecurity concept. Siemens' products and solutions constitute one element of plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsil for preventing unauthorized access to their plants, systems, machines and networks guentation) are in place. For additional information on industrial cybersecurity 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 strom 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 and no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens industrial Cybersecurity RSS Feed under https://www	 to web page: SiePortal 	https://sieportal.siemens.com/
• to website: Industry Online Support https://support.industry.siemens.com security information Siemens provides products and solutions with industrial cybersecurity function 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 responsil for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/c network segmentation) are in place. For additional information on industrial cybersecurity measures (bar and solutions undergo continuous development to make them more secure. Siemens strom 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 and to no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cet. (V4.7)	 to website: Image database 	https://www.automation.siemens.com/bilddb
security information Siemens provides products and solutions with industrial cybersecurity function 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 responsil for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a concect to an enterprise network or the internet if and to the extent such a connector necessary and only when appropriate security measures (e.g. firewalls and/c network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' product versions that ar no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	 to website: CAx-Download-Manager 	https://www.siemens.com/cax
security information Siemens provides products and solutions with industrial cybersecurity function 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 responsil for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/C 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 stror 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 an no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	 to website: Industry Online Support 	https://support.industry.siemens.com
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 responsil for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection 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 stror 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 an no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	ecurity information	
	security information	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
		subscribe to the Siemens Industrial Cybersecurity RSS Feed under

C C EG-Konf.	Declaration of Con- formity	UK CA	CCC		RCM
EMV	For use in hazardous	locations			
KC	K ATEX	IECEX	ЕM	<u>CCC-Ex</u>	
Marine / Shipping	Environment				
PRS	<u>Confirmation</u>				

8/22/2024 🖸