SIEMENS

Data sheet

6GK7545-1GX00-0XE0

product type designation



CP 1545-1

Communications processor CP 1545-1 for connection of SIMATIC S7-1500 to Industrial Ethernet; TCP/IP, UDP, S7 communication, security (VPN, firewall), SNMPv1/v3, DHCP, FTP client/server, email, IPv4/IPv6, time-of-day synchronization via NTP, connection to cloud systems via MQTT, 1x RJ45 (10/100/1000 Mbps).

transfer rate		
transfer rate		
at the 1st interface	10 1000 Mbit/s	
interfaces		
number of interfaces / according to Industrial Ethernet	1	
number of electrical connections		
at the 1st interface / according to Industrial Ethernet	1	
type of electrical connection		
 at the 1st interface / according to Industrial Ethernet 	RJ45 port	
supply voltage, current consumption, power loss		
type of voltage / of the supply voltage	DC	
supply voltage / 1 / from backplane bus	15 V	
relative symmetrical tolerance / at DC		
● at 15 V	3 %	
consumed current		
 from backplane bus / at DC / at 15 V / typical 	0.3 A	
power loss [W]	4.5 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 S7-1500 single width	
width	35 mm	
height	142 mm	
depth	129 mm	
net weight	0.32 kg	
fastening method		
S7-1500 rail mounting	Yes	
product features, product functions, product components / general		
number of units		
• per CPU / maximum	8	
• note	depending on CPU type	

product functions / cloud connectivity	
protocol / is supported	
Message Queuing Telemetry Transport (MQTT)	Yes
Advanced Message Queuing Protocol (AMQP)	No
product function / for cloud connectivity	
trigger management	Yes
time stamping	Yes
product feature / for cloud connectivity / buffered message	No
frame memory	
number of data points per device / maximum	500
performance data / open communication	
number of possible connections / for open communication	
by means of T blocks / maximum	118; depending on the system upper limit
data volume	
 as user data per ISO on TCP connection / for open communication / by means of T blocks / maximum 	65536 byte
number of Multicast stations	118
performance data / S7 communication	110
number of possible connections / for S7 communication	
maximum maximum	118: depending on the system upper limit
performance data / multi-protocol mode	118; depending on the system upper limit
	118
number of active connections / with multi-protocol mode	110
performance data / IT functions	
number of possible connections	22
as client / by means of FTP / maximum	32
as server / by means of FTP / maximum	16
number of possible connections	
as server / by means of HTTP / maximum	4
as email client / maximum	1
data volume / as user data for email / maximum	64 Kibyte
mantanina and a data / talaa antina	
performance data / telecontrol	
protocol / is supported	Ver-
protocol / is supported TCP/IP	Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering	
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support	Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported	Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported • SNMP v1	Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3	Yes Yes Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP	Yes Yes Yes Yes Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported • SNMP v1 • SNMP v3 • DCP • LLDP	Yes Yes Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported • SNMP v1 • SNMP v3 • DCP • LLDP configuration software	Yes Yes Yes Yes Yes Yes Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported • SNMP v1 • SNMP v3 • DCP • LLDP configuration software • required	Yes Yes Yes Yes Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function	Yes Yes Yes Yes Yes Yes Yes Yes Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information	Yes
protocol / is supported • TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported • SNMP v1 • SNMP v3 • DCP • LLDP configuration software • required identification & maintenance function • I&M0 - device-specific information • I&M1 - higher level designation/location designation	Yes Yes Yes Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information I&M1 - higher level designation/location designation product function / is supported / identification link	Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information I&M1 - higher level designation/location designation product functions / diagnostics	Yes Yes Yes Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes Yes Yes; acc. to IEC 61406-1:2022
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information I&M1 - higher level designation/location designation product function / is supported / identification link product functions / diagnostics product function / web-based diagnostics	Yes Yes Yes Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information I&M1 - higher level designation/location designation product function / is supported / identification link product functions / diagnostics product function / web-based diagnostics product functions / routing	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes Yes; acc. to IEC 61406-1:2022
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information I&M1 - higher level designation/location designation product function / is supported / identification link product functions / diagnostics product functions / routing service / routing / note	Yes Yes Yes Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes Yes Yes; acc. to IEC 61406-1:2022
protocol / is supported TCP/IP product functions / management, configuration, engineering product function / MIB support protocol / is supported SNMP v1 SNMP v3 DCP LLDP configuration software required identification & maintenance function I&M0 - device-specific information I&M1 - higher level designation/location designation product function / is supported / identification link product functions / diagnostics product functions / routing service / routing / note product function	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; via S7-1500 CPU IP routing up to 1 Mbps
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No
protocol / is supported	Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No No
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No No No
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No No No No
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No No No No No
protocol / is supported	Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes Yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No No No No No No
protocol / is supported	Yes Yes Yes Yes Yes Yes STEP 7 Professional V15.1 (TIA Portal) or higher Yes Yes Yes; acc. to IEC 61406-1:2022 Yes; via S7-1500 CPU IP routing up to 1 Mbps Yes No No No No No

No ROPP ROPE VAID DISC. ROPP ROPE VAID DISC. ROPP ROPE VAID DISC. ROPE VA	• VRRP	No
PROPE YAD DSL PROP PROPE VAD DSL No PROP VAD		
PPP PPP PPP PPP PPP PPP PPP PPP PPP P		
- PPGE via DSL roduct function / security freval version product function / with VPN connection ype of expropriate algorithms / with VPN connection ype of authentication procedure / with VPN connection Preshared key (PSK), X 509x3 certificates YPSK X 500x3 certificate		
Incomparison Inco		
firmed version stateful inspection product function / with VPN connection PF96 product function / with VPN connection PF96 product function product fun		
Product function / with VPM connection IPSec		stateful inspection
Spe of encryption algorithms / with VPN connection AES-266, AES-102, AES-102, AES-102, AES-366 State S		
bye of authentication procedure / with VPN connection bye of abasing aporthms / with VPN connection number of possible connections / with VPN connection number of possible connections / with VPN connection nection / with VPN connection / with VPN		
Speed finaling algorithms / with VPN connection MDS, SHA-1, SHA-256, SHA-384, SHA-512 number of possible connections / with VPN connection 16 product function password protection for VVeb applications No		
number of possible connections / with VPN connection product function		
ACL - IP-based or Pt-Crouting No ACL - IP-based for Pt-Crouting No According to ICL December No ACL - IP-based for ICL December No According to ICL December No According to ICL December No According to ICL B1346-2-2019 KEC According to ICL B1346-2-2019 According to ICL B1346-2-2019 According to ICL B1346-2-2019 According to		16
ACL - IP-based for PLC/routing ACL - IP-based for PLC/routing Act - IP-based for PLC/routing Act - IP-based for PLC/routing Act - IP-based for PLC-routing	product function	
No. Switch-off of non-required services Subclang of communication via physical ports No. I log file for unauthorized access Yes Troduct function / SICLOCK support Product function / SICLOCK support Product function / SICLOCK support Product function / Pass on time synchronization Product function / Pass on time synchronization Yes Product function / SICLOCK support No. Product function / Pass on time synchronization Yes Product function / Pass on time synchronization Yes Training / SICLOCK support No. No. Product function / Pass on time synchronization No. Product function / Pass on time synchronization No. No. Product function / Pass on time synchronization No. No. Product function / Pass on time synchronization No. Product function / Pass on time synchronization No. Product function / Pass on time synchronization Ves Indianal Product Declaration Significant on Approvals / Environmental Product Declaration Product function / Pass on time synchronization Ves Indianal Product Declaration Product function / Pass on time synchronization Product function / Pass on time synchronization Product function / Pass on time synchronization Ves Indianal Product Declaration Ves Indianal Product D	password protection for Web applications	No
Switch off of non-required services Diocking of communication with physical ports No log file for unauthorized access Pes product function / SICLOCK support product function / SICLOCK support Product function / SICLOCK support Product function / Sichock support NTP Pes Standards, specifications, approvals reference code according to IEC 81346-2:2019 KEC Standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Periodic function / Sichock support Author function / Sichock support Approvals / Certificates Periodic function / Sichock support No Pes Standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Periodic function / Pes Standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Periodic function / Pes Standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Pes Standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Pes Standards, specifications, approvals / Environmental Product Declaration Periodic function / Pes Standards, specifications, approvals / Environmental Product Declaration Periodic function / Pes Standards, specifications, approvals / Environmental Product Declaration International Product Declaration Pes Standards, specifications International Product Declaration Pes Standards, specifications International Product Declaration International Product Declara	ACL - IP-based	No
Blocking of communication via physical ports Ing file for unauthorized access Yes Product function / SICLOCK support Product function / Jess on time synchronization Product function / Jess on time synchronization Product function / Jess on time synchronization Yes Protocol / Is supported • NTP Yes Standards, specifications, approvals reference code • according to IEC 81346-2:2019 Standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Yes global warming potential (CO2 eq) • total • during manufacturing • during operation • after end of life • 0.35 kg further information / Internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industrial compose of the internet industrial cybersecurity functions that support industry siemens comminication • this silvanous amenins communication • this silvanous amenins communication • this website: Industrial communication • this website: Industrial communication • this website: Industrial communication • this silvanous amenins comminication •	ACL - IP-based for PLC/routing	No
No gried for unauthorized access product functions / gried / grie	switch-off of non-required services	Yes
product function / SICLOCK support product function / Jess on time synchronization Product function / Jess of time synchronization / Jess of time synchroni	 blocking of communication via physical ports 	No
product function / pass on time synchronization yes protocol / 1s supported NTP Yes standards, specifications, approvals reference code according to IEC 81346-2:2019 KEC standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration global warming potential (CO2 eq) • total • during aperation • during operation • during operation • after end of life other individual of the standards o	. , .	Yes
product function / pass on time synchronization NTP Yes standards, specifications, approvals reference code a coording to IEC 81346-2:2019 KEC standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Yes global warming potential (Co2 eq) total during manufacturing during operation after end of life 10.35 kg further information / Internet links internet link to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: CAx-Download-Manager to website: Industry Online Support thitss://swww.altomation.siemens.com/simatic.net thitss://swww.altomation.siemens.com/simatic.net thitss://swww.altomation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swew.automation.siemens.com/simatic.net thitss://swew.automation.siemens.com/simatic.n		
product function / pass on time synchronization NTP Yes standards, specifications, approvals reference code a coording to IEC 81346-2:2019 KEC standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Yes global warming potential (Co2 eq) total during manufacturing during operation after end of life 10.35 kg further information / Internet links internet link to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: CAx-Download-Manager to website: Industry Online Support thitss://swww.altomation.siemens.com/simatic.net thitss://swww.altomation.siemens.com/simatic.net thitss://swww.altomation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swww.automation.siemens.com/simatic.net thitss://swew.automation.siemens.com/simatic.net thitss://swew.automation.siemens.com/simatic.n	product function / SICLOCK support	No
• NTP Yes standards, specifications, approvals reference code • according to IEC 81346-2:2019 KEC standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration global warming potential (CO2 eq) • total • during munifacturing • during operation • after end of life • owebsite: Selection guide for cables and connectors • to web site: Selection guide for cables and connectors • to web page: Selection guide for cables and connectors • to web page: Selection guide for cables and connectors • to web page: Selection aid TIA Selection Toolol • to website: Industrial communication • to web page: Selection aid TIA Selection Toolol • to website: Industrial communication • to website: Industrial communication • to website: Industrial communication • 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 against cyber threats, it is necessary to implement—and continuously maintain—a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions onstitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks against cyber threats, it is necessary and only when appropriate security measures (e.g. firewalls and/or networks. Such systems, machines and networks against cyber threats, it is necessary or implement—and continuously maintain—a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions on the systems, machines and networks against cyber threats, it is necessary or implement and continuously maintain—a holistic, state-of-the-art industrial cybersecurity oncept. Siemens stron		Yes
reference code • according to IEC 81346-2-2019 KEC standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration global warming potential [COZ eq] • total • during aperation • after end of life • obsiste: Selection guide for cables and connectors • to website: Selection guide for cables and connectors • to website: Selection guide for cables and connectors • to website: Industrial communication • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • thiss://sieportal.siemens.com/ • thiss://sieportal.siemens.com/ **Sternens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks against oper threats, it is necessary to implement—and continuously amain —a holistic, state-of-the-art industrial cybersecurity functions networks and solutions constitute one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible one element of such a concept. Customers are responsible on element of such a concept. Customers are responsible on the latest product versions are used.	<u> </u>	
reference code according to IEC 81346-2:2019 KEC Environmental Product Declaration Pyes global warming potential [CO2 eq] total during operation after end of life outsite internet link to website: Selection guide for cables and connectors to web page: selection guide for cables and connectors to web page: selection guide for cables and connectors to web page: selection guide for cables and connectors to web page: selection and TIA Selection Tool to website: Industrial communication to website: Selection and TIA Selection Tool to website: Industrial communication to website: Selection and TIA Selection Tool to website: Industrial communication thitus://www.siemens.com/simatic-net thitus://www.siemens.com/simatic-net thitus://www.siemens.com/simatic-net thitus://siemens.com/cax thitus://siem	• NTP	Yes
* according to IEC 81346-2:2019 Standards, specifications, approvals / Environmental Product Declaration Product Declaration Yes	standards, specifications, approvals	
Environmental Product Declaration Environmental Product Declaration global warming potential [CO2 eq] • total • during manufacturing • during operation • after end of life • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support • thips://www.aubmation.siemens.com/simatic-net • thips://www.aubmation.siemens.com/simatic-net • thips://support.industry.siemens.com/ • thips://support.industry.siemens.com/ • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support • thips://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. In order to protect plants, systems, machines and networks. Such systems, machines and networks and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks such as connection is necessary and only when appropriate sevens are responsible for preventing unauthorized access to their plants, systems, anchines and networks against the appropriate sevens are responsible for preventing unauthorized access to their plants, systems, anchines and networks against the appropriate sevens are responsible for preventing unauthorized access to their plants, systems, machines and networks against set the appropriate sevens are responsible for preventing unauthorized access to their plants, systems, products and solutions undergo continuou	reference code	
global warming potential [CO2 eq] • total • during manufacturing • during poperation • after end of life • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: CAx-Download-Manager • 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. 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 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 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 enterprise network of 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 inf	 according to IEC 81346-2:2019 	KEC
e total • total • during manufacturing • during operation • during operation • after end of life 0.35 kg **Turther Information / Internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: Mage database • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: CAy-Download-Manager • to website: Thudustry Online Support **Turther Information **Security Information **Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, and networks, 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 networks and networks constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks capinst cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity measures (e.g. firevalls and/or networks systems, machines and networks or the internet and a conscious or networks or the internet and continuously maintain – a holistic, state-of-the-art industrial cybersecurity measures (e.g. firevalls and/or networks systems, machines and networks or the internet and a soon as they are available and that the latest product varions that are no longer supported, and failure to apply the latest 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 dyber theres. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert.V4.7) Approvals / Cortificat	standards, specifications, approvals / Environmental Product I	Declaration
• total • during manufacturing • during operation • during operation • after end of life • 0.35 kg **Turther information / internet links Internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to website: Industrial communication • 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 Security information Simmen sprovides 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 unautiforized access to their plants, systems, machines and networks against cyber threats, it is necessary and only when appropriate security measures (e.g. firevalls and/or networks. Such systems, machines and components should only be connected to an enterprise network or rich internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firevalls and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, place and to the extent such a connection is necessary and only when appropriate security measures (e.g. firevalls and/or networks segmentation) are place. For additional information on industrial cybersecurity measures that may be implemented, place as valiable and that the latest product updates are applied as soon as they are available and that the	Environmental Product Declaration	Yes
during manufacturing during operation after end of life	global warming potential [CO2 eq]	
during operation	• total	162.49 kg
after end of life internet link internet link internet link	during manufacturing	21.24 kg
internet link intern	 during operation 	140.9 kg
internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to web page: SiePortal • to website: Image database • to website: Industry Online Support • to website: Industry Online Support Security information Security information Security information Security information Security information Security information Silemens 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 as some parporpirate 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/cert. (V4.7) Approvals / Certificates	after end of life	0.35 kg
• to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industrial communication • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industry	further information / internet links	
to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal thttps://www.siemens.com/simatic-net thttps://sieportal.siemens.com/ thttps://sieportal.siemens.com/simatic-net thttps://sieportal.siemens.com/simatic-net thttps://sieportal.siemens.com/bilddb thttps://siemens.com/cax thttps://siemens.com/cax thttps://siemens.com/cax thttps://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)	internet link	
to website: Industrial communication to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support thttps://siemens.com/cax thttps://siemens.com/cax thttps://siemens.com/cax thttps://siemens.com/cax thttps://siemens.com/cax thttps://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) Approvals / Certificates	 to website: Selection guide for cables and connectors 	
to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://siemens.com/cax https://siemens.com/cax https://siemens.com/cax 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 and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such as systems, machines and one opports 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	 to web page: selection aid TIA Selection Tool 	https://www.siemens.com/tstcloud
to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://siemens.com/cax https://siemens.com/cax https://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) Approvals / Certificates	 to website: Industrial communication 	https://www.siemens.com/simatic-net
to twebsite: CAx-Download-Manager to twebsite: 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) Approvals / Certificates	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 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	to website: Image database	
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	<u> </u>	
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)	,	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 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	•	
Approvals / Certificates		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
General Product Approval For use in hazardous locations	Approvals / Certificates	
	General Product Approval	For use in hazardous locations













For use in hazardous locations

Environment

<u>FM</u>

CCC-Ex





Confirmation

last modified:

2/28/2025