6AG1208-0BA00-7AC2

Data sheet



SIPLUS NET SCALANCE XC208 based on 6GK5208-0BA00-2AC2 with conformal coating, -40...+70 °C, manageable layer 2 IE switch; 8x 10/100 Mbps RJ45 ports; 1x console port; diagnostics LEDs redundant power supply temperature range -40 °C to +70 °C; assembly: DIN rail/S7 mounting rail/wall office redundancy functions features (RSTP, VLAN,etc.); PROFINET IO device Ethernet/IP-compliant C-Plug slot;

product type designation	
product brand name	SIPLUS NET SCALANCE
product type designation	XC208
transfer rate	
transfer rate	10 Mbit/s, 100 Mbit/s
interfaces / for communication / integrated	
number of electrical connections	
 for network components or terminal equipment 	8; RJ45
number of 10/100 Mbit/s RJ45 ports	
with securing collar	8
interfaces / other	
number of electrical connections	
 for operator console 	1
 for signaling contact 	1
for power supply	1
type of electrical connection	
 for operator console 	RJ11
 for signaling contact 	2-pole terminal block
for power supply	4-pole terminal block
design of the removable storage	
• C-PLUG	Yes
operating voltage / of the signaling contacts	
at DC / rated value	24 V
operational current / of the signaling contacts	
at DC / maximum	0.1 A
supply voltage, current consumption, power loss	
type of voltage / 1 / of the supply voltage	DC
supply voltage / 1 / rated value	24 V
power loss [W] / 1 / rated value	4.2 W
supply voltage / 1 / rated value	9.6 31.2 V
ambient conditions	
ambient temperature / in horizontal mounting position / during operation	-40 +70 °C
installation altitude / at height above sea level / maximum	5000 m
relative humidity	
with condensation / according to IEC 60068-2-38 / maximum	100 %; RH including condensation/frost (no commissioning when condensation is present), horizontal installation
chemical resistance / to commercially available cooling lubricants	Yes; incl. airborne diesel and oil droplets
ambient condition / relating to ambient temperature - air pressure - installation altitude	Tmin Tmax at 1 140 hPa 795 hPa (-1 000 m +2 000 m) // Tmin (Tmax - 10 K) at 795 hPa 658 hPa (+2 000 m +3 500 m) // Tmin (Tmax - 20 K)

	at 658 hPa 540 hPa (+3 500 m +5 000 m)
resistance to biologically active substances	V 01 000 11 15 1 1 1 1 1 1 1 1 1 1 1 1 1
 conformity according to EN 60721-3-3 	Yes; Class 3B2 mold and fungal spores (excluding fauna); class 3B3 on request
 conformity according to EN 60721-3-6 	Yes; Class 6B2 mold, fungal and dry rot spores (excluding fauna)
resistance to chemically active substances	
• conformity according to EN 60721-3-3	Yes; Class 3C4 (RH < 75 %) incl. salt spray acc. to EN 60068-2-52 (severity degree 3); *
• conformity according to EN 60721-3-6	Yes; Class 6C3 (RH < 75%) incl. salt spray acc. to EN 60068-2-52 (Severity degree 3); *
resistance to mechanically active substances	
 conformity according to EN 60721-3-3 	Yes; Class 3S4 incl. sand, dust; *
 conformity according to EN 60721-3-6 	Yes; Class 6S3 incl. sand, dust; *
environmental category / according to IEC 60721 / note	* The supplied plug covers must remain in place on the unused interfaces during operation!
coating / for equipped printed circuit board / according to EN 61086	Yes; Class 2 for high availability
type of coating / protection against pollution according to EN 60664-3	Yes; protection of the type 1
type of test / of the coating / according to MIL-I-46058C	Yes; coating discoloration during service life possible
product conformity / of the coating / Qualification and Performance of Electrical Insulating Compound for Printed Board Assemblies according to IPC-CC-830A	Yes; conformal coating, class A
protection class IP	IP20
design, dimensions and weights	
design	compact
width	60 mm
height	147 mm
depth	125 mm
·	
net weight	0.52 kg
material / of the enclosure	Polycarbonate (PC-GF10) / pressure die cast aluminum
fastening method	Von
35 mm top hat DIN rail mounting well mounting	Yes
wall mounting G7 200 rail mounting	Yes Yes
S7-300 rail mountingS7-1500 rail mounting	Yes
product features, product functions, product components / ger	
cascading in the case of a redundant ring / at reconfiguration	50
time of <\~0.3\~s	
cascading in cases of star topology	any (depending only on signal propagation time)
	any (depending only on signal propagation time)
cascading in cases of star topology	any (depending only on signal propagation time) Yes
cascading in cases of star topology product function	
cascading in cases of star topology product function • QoS according to DSCP	
cascading in cases of star topology product function • QoS according to DSCP product feature	Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method	Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method	Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method product functions / management, configuration, engineering	Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method product functions / management, configuration, engineering product function	Yes No Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method product functions / management, configuration, engineering product function • CLI	Yes No Yes Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method product functions / management, configuration, engineering product function • CLI • web-based management	Yes No Yes Yes Yes
cascading in cases of star topology product function QoS according to DSCP product feature Cut Through switching method Store & Forward switching method product functions / management, configuration, engineering product function CLI web-based management MIB support	Yes No Yes Yes Yes Yes Yes
cascading in cases of star topology product function QoS according to DSCP product feature Cut Through switching method Store & Forward switching method product functions / management, configuration, engineering product function CLI web-based management MIB support TRAPs via email	Yes No Yes Yes Yes Yes Yes Yes Yes
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method product functions / management, configuration, engineering product function • CLI • web-based management • MIB support • TRAPs via email • configuration with STEP 7	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes
cascading in cases of star topology product function QoS according to DSCP product feature Cut Through switching method Store & Forward switching method product functions / management, configuration, engineering product function CLI web-based management MIB support TRAPs via email configuration with STEP 7 RMON	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye
cascading in cases of star topology product function	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye
cascading in cases of star topology product function QoS according to DSCP product feature Cut Through switching method Store & Forward switching method product functions / management, configuration, engineering product function CLI web-based management MIB support TRAPs via email configuration with STEP 7 RMON SMTP server	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes No Yes
cascading in cases of star topology product function QoS according to DSCP product feature Cut Through switching method Store & Forward switching method product functions / management, configuration, engineering product function CLI web-based management MIB support TRAPs via email configuration with STEP 7 RMON SMTP server port mirroring multiport mirroring CoS	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye
cascading in cases of star topology product function	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye
cascading in cases of star topology product function	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye
cascading in cases of star topology product function	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye
cascading in cases of star topology product function • QoS according to DSCP product feature • Cut Through switching method • Store & Forward switching method product functions / management, configuration, engineering product function • CLI • web-based management • MIB support • TRAPs via email • configuration with STEP 7 • RMON • SMTP server • port mirroring • multiport mirroring • CoS • PROFINET IO diagnosis • switch-managed	Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye

• HTTP	Yes
• HTTPS	Yes
• TFTP	Yes
• SFTP	Yes
• BOOTP	No
• GMRP	Yes
• DCP	Yes
• LLDP	Yes
EtherNet/IP	Yes
• SNMP v1	Yes
• SNMP v2	Yes
• SNMP v3	Yes
 IGMP (snooping/querier) 	Yes
identification & maintenance function	
I&M0 - device-specific information	Yes
I&M1 - higher level designation/location designation	Yes
product functions / diagnostics	
product functions / diagnostics	
·	Yes
port diagnostics actatictics Regulat Size	
statistics Packet Size statistics packet type	Yes
statistics packet type	Yes
• error statistics	Yes
• SysLog	Yes
product functions / VLAN	
product function	
 VLAN - port based 	Yes
 VLAN - protocol-based 	No No
VLAN - IP-based	No
number of VLANs / maximum	257
number of VLANs - dynamic / maximum	257
number of VLANs / at ring redundancy (HRP; MRP; standby	257
link)	
product functions / DHCP	
product functions / DHCP product function	
product functions / DHCP product function • DHCP server	Yes
product functions / DHCP product function • DHCP server • DHCP client	Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82	Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66	Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67	Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66	Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67	Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy	Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP)	Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy	Yes Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync	Yes Yes Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET	Yes Yes Yes Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy	Yes Yes Yes Yes Yes Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy • ring redundancy • high speed redundancy protocol (HRP) with redundancy	Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy • ring redundancy • ring redundancy • high speed redundancy protocol (HRP) with redundancy manager • high speed redundancy protocol (HRP) with standby	Yes Yes Yes Yes Yes Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy • ring redundancy • ring redundancy • high speed redundancy protocol (HRP) with redundancy manager • high speed redundancy protocol (HRP) with standby redundancy	Yes Yes Yes Yes Yes Yes Yes Yes Yes
product functions / DHCP product function • DHCP server • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy • ring redundancy • high speed redundancy protocol (HRP) with redundancy manager • high speed redundancy protocol (HRP) with standby redundancy • redundancy procedure STP	Yes Yes Yes Yes Yes Yes Yes Yes Ye
product functions / DHCP product function • DHCP server • DHCP client • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy • ring redundancy • high speed redundancy protocol (HRP) with redundancy manager • high speed redundancy protocol (HRP) with standby redundancy • redundancy procedure STP • redundancy procedure RSTP	Yes Yes Yes Yes Yes Yes Yes Yes Ye
product functions / DHCP product function • DHCP server • DHCP Option 82 • DHCP Option 66 • DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function • media redundancy protocol (MRP) with redundancy manager • of the PROFINET IO device / is supported / H-Sync forwarding • of the PROFINET IO device / is supported / PROFINET system redundancy • ring redundancy • high speed redundancy protocol (HRP) with redundancy manager • high speed redundancy protocol (HRP) with standby redundancy • redundancy procedure STP • redundancy procedure RSTP • redundancy procedure MSTP • Parallel Redundancy Protocol (PRP)/operation in the PRP-network • Parallel Redundancy Protocol (PRP)/Redundant Network	Yes Yes Yes Yes Yes Yes Yes Yes Ye
product functions / DHCP product function DHCP server DHCP Option 82 DHCP Option 66 DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function media redundancy protocol (MRP) with redundancy manager of the PROFINET IO device / is supported / H-Sync forwarding of the PROFINET IO device / is supported / PROFINET system redundancy ring redundancy ing redundancy high speed redundancy protocol (HRP) with redundancy manager high speed redundancy protocol (HRP) with standby redundancy redundancy redundancy procedure STP redundancy procedure RSTP redundancy procedure MSTP Parallel Redundancy Protocol (PRP)/operation in the PRP-network Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA)	Yes Yes Yes Yes Yes Yes Yes Yes Ye
product functions / DHCP product function DHCP server DHCP Option 82 DHCP Option 66 DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function media redundancy protocol (MRP) with redundancy manager of the PROFINET IO device / is supported / H-Sync forwarding of the PROFINET IO device / is supported / PROFINET system redundancy ining redundancy high speed redundancy protocol (HRP) with redundancy manager high speed redundancy protocol (HRP) with standby redundancy redundancy procedure STP redundancy procedure RSTP redundancy procedure MSTP Parallel Redundancy Protocol (PRP)/operation in the PRP-network Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA) passive listening	Yes Yes Yes Yes Yes Yes Yes Yes Ye
product functions / DHCP product function DHCP server DHCP Option 82 DHCP Option 66 DHCP Option 67 product functions / redundancy protocol / is supported / Media Redundancy Protocol (MRP) product function media redundancy protocol (MRP) with redundancy manager of the PROFINET IO device / is supported / H-Sync forwarding of the PROFINET IO device / is supported / PROFINET system redundancy ring redundancy ing redundancy high speed redundancy protocol (HRP) with redundancy manager high speed redundancy protocol (HRP) with standby redundancy redundancy redundancy procedure STP redundancy procedure RSTP redundancy procedure MSTP Parallel Redundancy Protocol (PRP)/operation in the PRP-network Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA)	Yes Yes Yes Yes Yes Yes Yes Yes Ye

product function configuration in RUN via CRRH-CIR product function *EEE 802.1x (radius) *RADUS deared *Post *Secretive* *Product function *EEE 802.1x (radius) *Post *RADUS deared *Post	system modification during operation	
product function EEE 802.1 \(\text{value} \) FARDIUS client Yes Foroadcastimulinast limiter Yes Foroadcast blooming Yes Foroadcast limiter blooming Yes Foroadcast functions / Imme Foroadcast functi	product function / configuration in RUN via CiR/H-CiR	Yes
EEEE ADC. 1x (radius) Yes	product functions / security	
RADIUS client Protocotal blocking Protocot // is supported SSH SSH SSL Yes SSL Yes SSL Yes Protocot function / films Protocot function SICLOCK support NPT-client SSTC SNP SNP SNP SNP Yes Protocot // is supported NPT-client Yes SNP SNP Yes Protocot // is supported NPT-client Yes SNP Yes SNRP Yes SNRP Yes SNRP Yes Sindiffications, approvals Continued of sulubility Coefficient of sulubility Coefficient of sulubility Standards, specifications, approvals Coefficient of sulubility Coefficient of sulubility Coefficient of sulubility Standards Solic interference emission For immunity to EMC Standards Specifications, approvals / other Certificate of sulubility After information in accordance with EM 50121-4 SRMS conding to IEC 81548-2 2015 Resident of Sulubility Standards Specifications approvals / other Certificate of sulubility Standards Specifications and Specifications approvals / other Certificate of sulubility Standards Specifications and Specifications approvals / other Certificate of sulubility Standards Specifications and Specifications approvals / other Certificate of sulubility Standards Specifications approvals / other Certifi	product function	
broadcast funitios dynical limiter broadcast blocking yes broadcast blocking yes sSH sNP sNP solic CoX support yes sNP sNP sNP sNP sNP sNP yes sNP sNP sNP sNP yes solic CoX support yes sNP sNP sNP yes solic CoX support yes sNP sNP sNP yes sNP sN	• IEEE 802.1x (radius)	Yes
Protect It is supported SSH Yes SSL Yes STOCKE Intention / filme product function / filme product function / filme product function / SICLOCK support SICLOCK support SSTP Client Yes SNTP client Yes SNTP Client SNTP Yes SNTP Yes SINTB YES	. ,	Yes
protect functions / time product function • SICL COR support • SICL Plant • SICL Pl	broadcast/multicast/unicast limiter	Yes
* SSH	 broadcast blocking 	Yes
roduct functions / time product functions / time product functions / time product functions / time product functions / time protect // support	protocol / is supported	
product functions / time product functions / Since - SICLOCK support - SITP client - SITP - SITTP - SIT	• SSH	Yes
product functions SICLOCK support SINTP client SINTP client SINTP client Yes Yes Yes Yes Yes Yes Yes Ye	• SSL	Yes
SICLOCK support NTP-client Yes SNTP total NTP SNTP SNTP SNTP SNTP **CE marking Product offerorimity according to EMC-guideline Standard **for EMC interference emission **for EMC interferen	product functions / time	
NTP client SNTP client NTP NTP SNTP Yes SANTP SANT	product function	
Protocol /s supported NTP SNTP SNTP STRP Pres Certificate of suitability Fres Standards Fres Fres Standards Fres Fres Fres Standards Fres Fre	 SICLOCK support 	Yes
protocol / is supported NTP NTP NTP NTP NTP NTP NTP NT	NTP-client	Yes
*NTP *SITP *SITP *SITP *Yes standards, specifications, approvals coefficiate of suitability *CE marking product conformity / according to EMC-guideline standard * for EMC interference emission * for immunity to EMC standards, specifications, approvals / other certificate of suitability *railway application in accordance with EN 50121-4 *RoHS conformity *Pes Product functions / general MTBF reference code * according to IEC 81346-2 * according to IEC 81346-2 * according to IEC 81346-2 * according to IEC 81346-2.2019 KFE *Internet link * to website. Selection guide for cables and connectors to web page. SelePortal * to website: Industrial communication * to website: Industrial communication * to website: Industry Online Support bitts://www.siemens.com/cs/ww/enview/109766358 bitts://www.siemens.com/cs/ww/envie	SNTP client	Yes
• SNTP Standards, specifications, approvals certificate of suitability • CE marking product conformity / according to EMC-guideline standard • for EMC interference emission • for immunity to EMC standards, specifications, approvals / other certificate of suitability • railway application in accordance with EN 50121-4 RoHS conformity • railway application in accordance with EN 50121-4 RoHS conformity product functions / general MTBF reference code • according to IEC 81346-2 • to website: Industrial communication • to web page: selection and TIA Selection Tool • to website: Industrial communication • to website: Industrial cyber security information Security information Security information Security information Security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. It is necessary to implement— and configuration and networks segmentation are industrial cybersecurity functions with reads. It is necessary to implement—and configuration or industrial cybersecurity functions with reads. It is necessary to implement—and configuration or industrial cybersecurity functions with reads. It is necessary to implement—and configuration or industrial cybersecurity functions with reads. It is necessary to implement—and configuration or industrial cybersecurity functions with reads. It is necessary to implement—and configuration	protocol / is supported	
setinificate of suitability		Yes
certificate of suitability • CE marking Product ordnormity / according to EMC-guideline standard • for EMC interference emission • for immunity to EMC standards, specifications, approvals / other certificate of suitability • callway application in accordance with EN 50121-4 • RoHS conformity product functions / general MTBF reference code • according to IEC 81346-2 • according to IEC 81346-2:2019 KFE further information / internet links internet link • to website: Selection guide for cables and connectors • to website: Industrial communication • to website: Industrial communication • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support security information Secur	• SNTP	Yes
product conformity / according to EMC-guideline standard • for EMC Interference emission • for immunity to EMC • retificate of suitability • railway application in accordance with EN 50121-4 • RoRS conformity • railway application in accordance with EN 50121-4 • RoRS conformity • realway application in accordance with EN 50121-4 • RoRS conformity • reduct functions / general MTBF 48 a reference code • according to IEC 81346-2 • according to IEC 81346-2:2019 KFE 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: Image database • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support Security information Security information Security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain — a hotistic note of the proporties security information and in a management of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics and solutions constitute one element of such a concept. Customics	standards, specifications, approvals	
standard • for EMC interference emission • for immunity to EMC tandards, specifications, approvals / other certificate of suitability • railway application in accordance with EN 50121-4 • RoHS conformity • railway application in accordance with EN 50121-4 • RoHS conformity • reference code • according to IEC 81346-2 • to website: Selection guide for cables and connectors • to website: Selection guide for cables and connectors • to website: Industrial communication • to website: Industrial communication • to website: Industrial communication • to website: Industrial conformation of this substite: CAA-Download-Manager • to website: Industrial condord-Manager	certificate of suitability	
standard • for EMC interference emission • for immunity to EMC standards, specifications, approvals / other certificate of suitability • railway application in accordance with EN 50121-4 • RoHS conformity • railway application in accordance with EN 50121-4 • RoHS conformity • railway application in accordance with EN 50121-4 • RoHS conformity • Yes product functions / general MTBF reference code • according to IEC 81346-2 • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industry Online Support • to website: Industry Online Support • to website: Industry Online Support • thitss://www.siemens.com/simalic-net • thitss://support.industry.siemens.com/simalic-net • thitss://support.industry.	CE marking	Yes
For EMC interference emission For immunity to EMC EN 81000-6-2, EN 50121-4 EN 81000-8-3, EN 50121-4 EN 81000-8-4, EN 50121-4 EN 81000-8-4, EN 50121-4 EN 81000-8-2, EN 50121-4 EN 81000-8-	product conformity / according to EMC-guideline	2014/30/EU
• for immunity to EMC standards, specifications, approvals / other certificate of suitability • railway application in accordance with EN 50121-4 • RoHS conformity MTBF 48 a reference code • according to IEC 81346-2 • according to IEC 81346-2 • according to IEC 81346-2 • according to IEC 81346-2 KFE 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: Industry Online Support • to website: Industrial ophersecurity Concept. Slemens products and solutions on industrial ophersecurity concept. Slemens products and solutions on industrial ophersecurity concept. Slemens products and solutions constitute on concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks against opher network segmentation on industrial oph	standard	
certificate of suitability • railway application in accordance with EN 50121-4 • Rolf-S conformity * respectively application in accordance with EN 50121-4 • Rolf-S conformity * Yes * reference code • according to IEC 81346-2 • according to IEC 81346-2:2019 * KFE * further information / 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 • to website: Industry Online Support * thttps://www.siemens.com/cax * https://www.siemens.com/cax * https://www.siemens.com/ca	 for EMC interference emission 	EN 61000-6-4, EN 50121-4
certificate of suitability • railway application in accordance with EN 50121-4 • ROHS conformity **Tes** **ROHS conformity **Tes**	 for immunity to EMC 	EN 61000-6-2, EN 50121-4
RoHS conformity Product functions / general MTBF	standards, specifications, approvals / other	
Product functions / general MTBF 48 a reference code • according to IEC 81346-2 • according to IEC 81346-2 • type 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: Image database • to website: Image database • to website: Image database • to website: Industry online Support • to website: Industry online Support industry siemens.com/cax • thitps://www.siemens.com/cax • thitps://www.si	certificate of suitability	
mTBF reference code a according to IEC 81346-2 to the website: Selection guide for cables and connectors to web site: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web site: Industrial communication to website: CAx-Download-Manager to website: CAx-Download-Manager thtps://www.siemens.com/simatic.net thtps://www.simatic.net thtps://www.simatic.net thtps://www.simatic.net thtps://www.siemens.com/simatic.net thtps://www.simatic.net thtps://www.	 railway application in accordance with EN 50121-4 	Yes
reference code	RoHS conformity	Yes
reference code according to IEC 81346-2:2019 KF 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: Industry Online Support • to website: Industry Online Support Security information Industrial information 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. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks against cyber security information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens brongly recommends that product updates are applied as soon as they are available and that the latest product versions state 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	product functions / general	
according to IEC 81346-2.2019 Further information / Internet links internet link a to website: Selection guide for cables and connectors a to web page: selection aid TIA Selection Tool b to website: Industrial communication a to website: Industrial communication b to website: Industrial communication b to website: Image database b to website: Image database b to website: Industry Online Support b type://www.siemens.com/cs/ b type://support.industry.siemens.com/ security information security information security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to nontinuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and onopnonents 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 networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and	MTBF	48 a
according to IEC 81346-2:2019 further information / internet links internet link a to website: Selection guide for cables and connectors b to web page: selection aid TIA Selection Tool a to website: Industrial communication b to website: Image database a to website: CAx-Download-Manager b to website: Industry Online Support b thtps://www.automation.siemens.com/bilddb https://www.automation.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. In order to protect plants, 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 (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' product sand 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 updates, subscribe to the Siemens latest updates may informed about product updates, subscribe to the Siemens latest updates may informed about product updates, subscribe to the Siemens latest updates are information on industrial cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed un	reference code	
internet link • to website: Selection guide for cables and connectors • to web page: selection and TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • to website: Industrial of phase, 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 envorks against solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, 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	•	KF
internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web page: SiePortal • to website: Inage database • 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. Customers are responsible for preventing unautirized access to their plants, systems, machines and networks. Such systems, machines and onetworks. Such systems, machines and onetworks. Such systems, machines and networks 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. Giemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product updates, subscribe to the Siemen Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)		KFE
in to website: Selection guide for cables and connectors in to web page: selection aid TIA Selection Tool in to website: Industrial communication in to web page: SiePortal intps://www.siemens.com/simatic-net intps://sieportal.siemens.com/ intps://sieportal.siemens.com/ intps://www.siemens.com/simatic-net intps://www.siemens.com	further information / internet links	
to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal to web page: SiePortal to website: Image database https://www.siemens.com/simatic-net to website: CAx-Download-Manager to website: Industry Online Support thtps://www.siemens.com/cax to website: Industry Online Support security information security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, enachines 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 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 and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems machines and networks. 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)	•	The state of the s
to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: CAx-Download-Manager to website: Industry Online Support Security information Security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	. •	
to to website: Image database to to website: CAx-Download-Manager to 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 one promoted to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a 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 ma		
• to website: CAx-Download-Manager • to website: Industry Online Support **https://support.industry.siemens.com/ **security information **Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	. •	
• to website: 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)		
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)	9	
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)	security information	
	Scounty information	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

General Product Approval

EMV

Manufacturer Declaration UK



Miscellaneous



last modified: 7/24/2024 🖸