SIEMENS

Data sheet

6GK5328-4TS01-2EC2



SCALANCE XCH328 managed layer 2 IE switch, 24x 10/100/1000 Mbps RJ45, 4x 1/10 Gbps SFP+ port, LED diagnostics,error signaling contact with select/set pushbutton, PROFINET IO device, network management, redundancy functions, office features (RSTP, VLAN, IGMP,..) CLP included in scope of supply assembly: DIN rail/S7 mounting rail conformal coating

product type designation	
product brand name	SCALANCE
transfer rate	
transfer rate	10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s
interfaces / for communication / integrated	
number of electrical connections	
 for network components or terminal equipment 	24; RJ45
number of 10/100/1000 Mbit/s RJ45 ports	
with securing collar	24
number of electrical connections	
• for SFP+	4; 1000 Mbps and 10000 Mbps SFP usable
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 	USB (2.0 Port, Type B, serial via USB)
 for signaling contact 	2-pole terminal block
for power supply	2 x 2-pin terminal block
design of the removable storage	
• CLP	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	
product component / connection for redundant voltage supply	Yes
type of voltage / 1 / of the supply voltage	DC
 supply voltage / 1 / rated value 	24 V
 power loss [W] / 1 / rated value 	43.2 W
 supply voltage / 1 / rated value 	19.2 28.8 V
 consumed current / 1 / maximum 	1.8 A
 type of electrical connection / 1 / for power supply 	2 x 2-pole terminal block
 product component / 1 / fusing at power supply input 	Yes
fuse protection type / 1 / at input for supply voltage	F 10 A / 250V
ambient conditions	
ambient temperature	
during operation	-40 +60 °C
 during storage 	-40 +85 °C



9/26/2024

during transport	-40 +85 °C
relative humidity	
at 25 °C / without condensation / during operation /	95 %
maximum	
operating condition / fanless operation	Yes
protection class IP	IP20
design, dimensions and weights	
design	compact
width	210 mm
height	147 mm
depth	125 mm
net weight	1.9 kg
fastening method	
• 19-inch installation	No
 35 mm top hat DIN rail mounting 	Yes
wall mounting	Yes
 S7-300 rail mounting 	Yes
● S7-1500 rail mounting	Yes
product functions / management, configuration, engineering	
product function	
• CLI	Yes
 web-based management 	Yes
MIB support	Yes
TRAPs via email	Yes
 configuration with STEP 7 	Yes
RMON	No
• port mirroring	Yes
multiport mirroring	Yes
 Encapsulated Remote Traffic Mirroring (ERTM) 	Yes
• CoS	Yes
 PROFINET IO diagnosis 	Yes
 switch-managed 	Yes
PROFINET conformity class	В
telegram length / for Ethernet / maximum	1632 byte
protocol / is supported	
• Telnet	No
• HTTP	Yes
• HTTPS	Yes
• TFTP	Yes
• FTP	Yes
• SFTP	Yes
BOOTP NETCONF	Yes
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 function	
port diagnostics	Yes
statistics Packet Size	Yes
statistics packet type	Yes
error statistics	Yes
• SysLog	Yes



9/26/2024

product functions / VLAN	
product function	
VLAN - port based	Yes
VLAN - protocol-based	No
• VLAN - IP-based	No
VLAN dynamic	Yes
number of VLANs / maximum	512
number of VLANs - dynamic / maximum	512
product functions / DHCP	
product function	
DHCP server	No
DHCP client	Yes
DHCP Option 82	No
DHCP Option 66	Yes
DHCP Option 67	Yes
product functions / redundancy	
protocol / is supported / Media Redundancy Protocol (MRP)	Yes
product function	
media redundancy protocol (MRP) with redundancy manager	Yes
Media Redundancy Protocol Interconnection (MRP-I)	No
ring redundancy	Yes
 high speed redundancy protocol (HRP) with redundancy manager 	No
 high speed redundancy protocol (HRP) with standby redundancy 	No
redundancy procedure STP	Yes
redundancy procedure RSTP	Yes
 redundancy procedure RSTP+ 	Yes
redundancy procedure MSTP	Yes
passive listening	No
• eRSTP	Yes
protocol / is supported	
• LACP	No
product functions / security	
protocol / is supported	
• RADIUS	Yes
• SSH	Yes
• SSL	Yes
product functions / time	
product function	
SICLOCK support	Yes
NTP-client	Yes
IEEE 1588 v2 transparent forwarding	Yes
protocol / is supported	
• NTP	Yes
IEEE 1588 profile default	Yes
standards, specifications, approvals	
certificate of suitability	
• CE marking	Yes
UKCA marking	Yes
• cULus approval	Yes
• KC approval	Yes
Regulatory Compliance Mark (RCM)	Yes
product conformity / according to EMC-guideline	2014/30/EU
standard	
for EMC interference emission	EN 61000-6-4
• for immunity to EMC	EN 61000-6-2
for safety / from CSA and UL	UL 60950-1 E115352, UL-61010-2 E85972
standards, specifications, approvals / hazardous environments	
certificate of suitability	
-	



• UKEXYes• ECEXYes• CCC / for hazerdous zone according to GB standardYes• CCC / for hazerdous zone according to GB standardYes• For registrationYes• Certifications, approvals / otherYescertificate of subbilityYes, use only in areas not accessible to the public• allway application in accordance with EN 50121-4Yes, use only in areas not accessible to the public• allway application in accordance with EN 50125-3Yes• Texcury for induction automation systems / according to ECGYes• Conduct Declaroting, approvals / Environmental Product DeclarotionYes• Global Warming Potential [CO2 eq]124/4 3 kg• other122/3 kg• other122/3 kg• other122/3 kg• other15.6 areference codeKF• occording to ECG 313/6-2KF• occording to ECG 313/6-2KF• other15.6 areference codeKF• otherNewbalts: Selection guide for cables and connectors• to websits: Selection guide for cables and connectorsInter/surgoot Industry semens condicional/New View/100765358• to websits: Industration communicationInter/surgoot Industry semens condicional/New View/10		
 Cirkin Cirkin Cir	• ATEX	Yes
• Unable de genovel Yes • De de Corton bazardous sone according to GB standard Yes • Service de Corton bazardous sone according to GB standard Yes • Service de Corton bazardous sone according to GB standard Yes • Service de Corton bazardous sone according to GB standard Yes • Service de Corton bazardous sonte He M 1012-16 Yes • Service de Corton bazardous sonte He M 1012-16 Yes • Service de Corton bazardous sonte He M 1012-16 Yes • Service de Corton bazardous sonte de Corton He M 1012-16 Yes • Service de Corton bazardous sonte de Corton He M 1012-16 Yes • Service de Corton bazardous sonte de Corton He M 1012-16 Yes • Service de Corton Bazardous Sonte de Corton He M 1012-16 Yes • Service de Corton Bazardous Sonte de Corton He M 1012-16 Yes • Service de Corton Bazardous Sonte de Corton He M 1012-16 Yes • Service de Corton He M 1012-16 Yes •		
 even specifications, approvals of other standard in the specification of approvals of other standards. Specifications approvals approvals of other standards. Specifications approvals of other standards. Specification approvals of other standards. Specifications approvals of oth		
• Progetation Yes tankarder, specifications, spectrake statistics Ves • entivery equivalence in the scorednese with EN 901214 Yes, use only in areas not accessible to the public • entivery equivalence in accordnese with EN 901214 Yes, use only in areas not accessible to the public • entivery equivalence in accordnese with EN 901214 Yes • entivery equivalence in accordnese with EN 901214 Yes • entivery equivalence in accordnese with EN 901214 Yes • entivery equivalence in accordnese with EN 901214 Yes • entivery equivalence in accordnese with EN 901214 Yes • entivery equivalence in accordnese in the scordnese in the score in the sco		
standards, spudifications, approvals / other certificated of suitability railway application in accordance with EN 60125-3 Yes, use only in areas not accessible to the public Treativity for induction at approvals / Environmental Product Declaration Environmental Poduct Declaration Environmental Poduct Declaration Order and the environmental Poduct Declaration Environmental Poduct Declaration Order and the environmental Poduct Declaration Environmental Poduct Declaration Order and the environmental Poduct Declaration Order and the environmental Poduct Declaration Order and the environmental Poduct Declaration Terrestrict For induct Declaration Order and the environmental Poduct Declaration MTEF Terrestrict For induct Declaration March Potential (SOC ed) • according to EC 81346-2 • b website: Selection guide for cables and connectors • b website: Induction of induction o	-	
eerificate of suitability erilavay application in accordance with EN 501214 Yes Yes Yes Yes Yes Ves Ves Ves	, , , , , , , , , , , , , , , , , , ,	
A sharey application in accordance with EN 501214 Yes		
• aniway application in accordinge with P 50125-3 Yes • Casa-2-2 control Yes <td></td> <td>Very use only in proce not accessible to the public</td>		Very use only in proce not accessible to the public
Precury for inducting attornation systems / according to IEC Yes Standards, specifications, approvals / Environmental Product Declaration Yes Environmental Product Declaration Yes Oldolal Wenning Potential (C2 eq) 124.4 3 kg • otalig manufacturing 122.74 kg • otalig operation 122.74 kg • otalig operation 126.6 a • otalig operation 15.6 a • occording to IEC 81346-2.2019 KFE • otalig operation / Internet links 15.6 a • overbasitic Solection guide for cables and connectors Interview information / Internet links • overbasitic Solection guide for cables and connectors Interview information / Internet links • overbasitic Industry online Support Interview information / Interview information		
B2443-422019 Interview of the second status of		
Environmental Product Declaration Yes Global Warming Potential (CO2 eq) 1244.3 kg • I data 122.74 kg • during annufacturing 122.74 kg • during operation 0.11 kg • order functions / general MTEF reference code		Tes
Global Warming Potential (CO2 eq) 1244.3 kg • Loting manufacturing • Loting • Loting manufacturing • Loting	standards, specifications, approvals / Environmental Product D	eclaration
 total total ider and allawing ider allawing<!--</td--><td>Environmental Product Declaration</td><td>Yes</td>	Environmental Product Declaration	Yes
 e. during manufacturing e. during operation e. during operat	Global Warming Potential [CO2 eq]	
 e. during operation e. during operation e. during of effect of sides e. during of effect of sides e. during to IEC 81346-2 e. during to IEC 8134	total	1244.3 kg
	 during manufacturing 	122.74 kg
Product functions / general 15.6 a MTEF 15.6 a reference code according to IEC 81346-2 according to IEC 81346-2.2019 KFE Warranty period 5 a utreber Information / Internet links internet link internet link executing to IEC 81346-2.2019 is web page: selection guide for cables and connectors https://www.siemens.com/tsticuid is web page: selection aid TA Selection Tool https://www.siemens.com/tsticuid is web page: selection aid TA Selection Tool https://www.siemens.com/tsticuid is website: industrial communication https://www.siemens.com/tsticuid is website: industry Online Support https://www.siemens.com/tsticuid of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber treats, it is necessary to implement – and continuously maintian – a holistic, state-64-the-art industrial cybersecurity unclones security information Siemens provides products and solutions with industrial cybersecurity measures that augopt industry. Siemens and networks against cyber treats, it is necessary to implement – and continuously maintian – a holistic, state-64-the-art industrial cybersecurity indomnes and networks and a connector tybersecurity indomstres and contheoremes convector the intenet find to the	during operation	1120.64 kg
MTBF 15.6 a reference code according to IEC 81346-2 according to IEC 81346-2.2019 KFE scanding to IEC 81346-2.2019 KFE to website: Selection guide for cables and connectors io web page: selection aid TIA Selection Tod to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: CAx-Downland-Manager to website: Industrial comport to website: Industrial comport security information security information security informatin security information	after end of life	0.91 kg
Interference code Interview excoording to IEC 81346-2 KF accoording to IEC 81346-2.2019 KFE Warrany period 5 a urther information / informet links Interview in website:: Selection guide for cables and connectors: hubs://www.siemens.com/skow/en/view/109766358 io website:: Intage database hubs://www.siemens.com/simult-rule io website:: Industry addition operation hubs://www.siemens.com/simult-rule io website:: Industry on In Support bits://www.siemens.com/simult-rule io website:: Industry on In Support bits://www.siemens.com/simult-rule bewebsite:: Industry on In Support bits://www.siemens.com/simult-rule bewebsite: Industry on In Support bits://www.siemens.com/simult-rule bewebsite: Industry on Interview Security information security information Security information of plans, system, machines and networks against cyber in order to protect plans, system, machines and networks against cyber in order to protect plans, system, machines and networks against cyber in order to protect plans, system, machines and networks against cyber in order to protect plans, system, machines and networks against cyber in order to protect plans, systements on order to protect p	product functions / general	
According to EC 81346-2 KF According to EC 81346-2/2019 KF Warranty period 5 a Unter Information / Internet links Hitss://augoort.industry.siemens.com/cs/ww/en/vjew/108768358 Internet link Hitss://augoort.industry.siemens.com/cs/ww/en/vjew/108768358 Io website: Selection guide for cables and connectors Hitss://www.siemens.com/similio.net Io website: Selection guide for cables and connectors Hitss://www.siemens.com/similio.net Io website: Industrial communication Hitss://www.siemens.com/similio.net Io website: Industry Online Support Hitss://www.siemens.com/similio.net Security information Stenens provides products and solutions with industrial cybersecurity functions security information Stenens provides products and solutions with industrial cybersecurity functions state-of-the-art industrial cybersecurity concept. Customers are responsible for protect plants, systems, machines and networks and solutions with industrial - a holistic, state-of-the-art industrial cybersecurity concept. Customers are responsible for protect plants, systems, machines and networks and solutions on the internet if and to be extent sub-4 a connection on concessary and only when appropriate security measures (e.g. firewals and/or networks and solutions with industry. Siemens products and solutions with industry. Siemens products and solutions on the internet if and to be extent sub-4 a connection on concessary and only when appropriate security measures (e.g. firewals and/or		15.6 a
excording to EC 81346-2:2019 KFE Warranty period 5 a the second of t	reference code	
eccording to EC 81348-2:2019 Warrary period Sa Control protect Protect Information / Internet links encode protect Protec	 according to IEC 81346-2 	KF
further information / internet links interret link • to website: Selection guide for cables and connectors • to web page: selection aid TA Selection Tool • to website: Industrial communication • to website: Industrial communication • to website: CAx-Download-Manager • to website: Industry Online Support • to website: Industry Online Support security information secoverty information on tooperation seconces	• according to IEC 81346-2:2019	KFE
internet link • to website: Selection guide for cables and connectors • to web page: selection at TIA Selection Tool • to website: Industrial communication security information security information security information security information security information excurity information security information se	Warranty period	5 a
internet link • to website: Selection guide for cables and connectors • to web page: selection at TIA Selection Tool • to website: Industrial communication security information security information security information security information security information excurity information security information se		
 howeb page: selection and TIA Selection Tool howeb page: selection and the tabulation selemens com/bild/db howeb site: industry Online Support security information security informat	internet link	
 h web page: selection aid TIA Selection Tod h website: industrial communication h website: industrial communication h website: industrial communication h website: CAx-Download-Manager h to website: industry Online Support h web	 to website: Selection guide for cables and connectors 	https://support.industry.siemens.com/cs/ww/en/view/109766358
 https://seportal.siemens.com/ https://seportal.siemens.com/biddb https://www.siemens.com/biddb https:/	-	https://www.siemens.com/tstcloud
• to website: Image database https://www.automation_siemens.com/bilddb • to website: Industry Online Support https://www.siemens.com/cax security information https://www.siemens.com/cax 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 with industrial - a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions with industrial - a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate access to their plants, systems, machines and networks and solutions connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate access to their plants, systems, machines and onetworks and solutions controluces development to make them more secure. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threast. To stay informed about product updates, subscribe to the Siemens. Industrial Cybersecurity RSS Feed under this/s//www.siemens.com/cet. (V.4.7)	to website: Industrial communication	https://www.siemens.com/simatic-net
• to website: Image database https://www.automation.siemens.com/bildbb • to website: Ax-Download-Manager https://www.siemens.com/cax • to website: Industry Online Support https://www.siemens.com/cax security information security information security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Ustomers are responsible for preventing unauthorized access to their plants, systems, machines and networks and solutions on industrial – a holistic, state-of-the-art industrial cybersecurity concept. Ustomers are responsible for preventing unauthorized access to their plants, systems, machines and networks and solutions controluced velopment to and to the extent such a connection is necessary and only where averalized 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/cet.ustomers Approvals / Certificates Declaration of Contertor family For use in hazardous locations Externel Declaration of Contertor formity For formity Mage For For	 to web page: SiePortal 	https://sieportal.siemens.com/
https://www.siemens.com/cax https://support.industry_siemens.com/cax security information Security informating security information on induce </td <td></td> <td>https://www.automation.siemens.com/bilddb</td>		https://www.automation.siemens.com/bilddb
• 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 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. Such systems, machines and networks such a solutions constitute one element of such a concept. Customers are responsible in creworks. Such systems, machines and networks or the internet if and to the extent such a connection is necessary and only when appropriate security measures that an gone threat such a connection is necessary and only when appropriate security measures that may be implemented, please wisit www.siemens.com/cet.customers are responsible and that the latest product supported. and future to apply the latest updates may 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 future to apply the latest updates may product and solutions cuberier to the Siemens inductive to applied as soon as they are available to be latest on the site or byter threats. To stay informed about product updates, subscribe to the Siemens inductive to applied as soon as they are available and that the latest product versions are used. Use of product versions that are to spece threats. To stay informed about product updates, subscribe to the Siemens inductive to apply the data to the sieme in the size of t	-	
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 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 industrial cybersecurity reasures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity industrial cybersecurity reasures (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/cyt.(V4.7) Approvals / Certificates For use in hazardous locations General Product Approval For use in hazardous locations EM Declaration of Conformity formity Image Conformity formity	to website: Industry Online Support	https://support.industry.siemens.com
that support the secure operation of plants, systems, machines and networks in order to protect plants, systems, machines and networks state-of-the-art industrial cybersecurity concept. Sustemers 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 such a continuous) we implement—d please visit www.siemens.com/cybersecurity measures (e.g. firewalls and/or networks such are propriate security measures (e.g. firewalls and/or network such a content of and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network such acconnect that may be implemented, please visit www.siemens.com/cybersecurity measures (the grad such 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 Stemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates For use in hazardous locations General Product Approval EM Declaration of Conformity formity formity Experiment formity Experiment formity Em beclaration of Conformity formity formity formity <td>security information</td> <td></td>	security information	
General Product Approval For use in hazardous locations Declaration of Con- formity UK formity FM UV	security 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
	A source la / Contification	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
		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)
	General Product Approval	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)
	General Product Approval	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)
Test Certificates Environment Industrial Communication	General Product Approval	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)
Test Certificates Environment Industrial Communication	General Product Approval	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)
	General Product Approval	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)
	General Product Approval	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) For use in hazardous locations



Type Test Certific-ates/Test Report



PROFINET

last modified:

8/22/2024 🖸

