Data sheet

6GK5208-0HA10-2ES6



SCALANCE XP208EEC, IP65, managed layer 2 IE switch, railway approval, 6x 10/100 Mbps, 2x 1000 Mbps, M12 ports, LED diagnostics, error signaling contact, redundant power supply, PROFINET IO device, network management, can be operated in redundant ring, dust caps, including -40 °C to +70 °C, C-PLUG optional.

product type designation		
product brand name	SCALANCE	
product type designation	XP208EEC	
transfer rate		
transfer rate	10 Mbit/s, 100 Mbit/s, 1000 Mbit/s	
interfaces / for communication / integrated		
number of electrical connections		
 for network components or terminal equipment 	8; M12	
number of 10/100 Mbit/s M12-ports (D-coded)	6	
number of 10/100/1000 Mbit/s M12-ports (X-coded)	2	
interfaces / other		
number of electrical connections		
 for operator console 	1	
for signaling contact	1	
for power supply	2	
type of electrical connection		
 for operator console 	5 pin M12 socket (A coded)	
 for signaling contact 	5-pin M12 connector (B-coded)	
• for power supply	4-pole M12 plug (L-coded)	
design of the removable storage		
• C-PLUG	Yes	
product function / device replacement with replacement of the storage medium	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; XP-200EEC with EN 50155 supports the voltage range 16.8 31.2 V DC	
power loss [W] / 1 / rated value	4.8 W	
 consumed current / 1 / at rated supply voltage / maximum 	0.2 A	
 supply voltage / 1 / rated value 	19.2 31.2 V	
consumed current / 1 / maximum	0.2 A	
 type of electrical connection / 1 / for power supply 	4-pole M12 plug (L-coded)	
 product component / 1 / fusing at power supply input 	Yes	
fuse protection type / 1 / at input for supply voltage	4 A / 60 V	
ambient conditions		
ambient temperature		

during operation	-40 +70 °C
during operation during storage	-40 +70 °C
during storage during transport	-40 +85 °C
during transport	EEC variants with EN 50155 support for 10 minutes: +85 °C
note relative humidity	LEO Varianto with EN 30100 support for 10 milliones. 700 C
at 25 °C / without condensation / during operation /	95 %
maximum	33 /0
protection class IP	IP65
design, dimensions and weights	
design	compact
width	200 mm
height	200 mm
depth	49 mm
net weight	1.8 kg
product feature / conformal coating	Yes
material / of the enclosure	Aluminum
fastening method	module rack mounting, back wall mounting
wall mounting	Yes
product features, product functions, product components / gene	eral
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)
product function	
QoS according to DSCP	Yes
product feature	M-
Cut Through switching method Stage & Facuus devitabiling method	No Voc
Store & Forward switching method	Yes
product functions / management, configuration, engineering	
product function	V.
• CLI	Yes
web-based management	Yes
MIB support	Yes
• TRAPs via email	Yes
• configuration with STEP 7	Yes
• RMON	Yes
SMTP server	No
• port mirroring	Yes
multiport mirroring	Yes
• CoS	Yes
with IRT / PROFINET IO switch PROFINET IO discression.	No Voc
PROFINET IO diagnosis	Yes
switch-managed PROFINET and formity class	Yes
PROFINET conformity class	B
network load class / according to PROFINET	3 40240 byte
telegram length / for Ethernet / maximum	10240 byte
protocol / is supported	Voe
TelnetHTTP	Yes
	Yes
HTTPS TFTP	Yes Yes
SFTP BOOTP	Yes No
• BOOTP • GMRP	Yes
DCP	Yes
• DCP • LLDP	Yes
• EtherNet/IP	Yes
• SNMP v1	Yes
• SNMP v2	Yes
SNMP v3 ICMP (specifical/queries)	Yes
IGMP (snooping/querier) identification 9 maintageness function	Yes
identification & maintenance function	

- 19 MO device execific information	Voc
I&M0 - device-specific information I&M1 - higher level designation/legation designation	Yes Yes
I&M1 - higher level designation/location designation product functions / diagnostics	165
product functions r diagnostics	
port diagnostics	Yes
statistics Packet Size	Yes
statistics racket type	Yes
error statistics	Yes
SysLog	Yes
product functions / VLAN	
product function	
VLAN - port based	Yes
VLAN - protocol-based	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 function • DHCP server	Yes
DHCP server DHCP client	Yes
DHCP Option 82	Yes
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	Yes
manager	
 Media Redundancy Protocol Interconnection (MRP-I) 	Yes
 of the PROFINET IO device / is supported / H-Sync forwarding 	Yes
of the PROFINET IO device / is supported / PROFINET system redundancy	Yes
• ring redundancy	Yes
 high speed redundancy protocol (HRP) with redundancy manager 	Yes
 high speed redundancy protocol (HRP) with standby redundancy 	Yes
 redundancy procedure STP 	Yes
redundancy procedure RSTP	Yes
redundancy procedure RSTP+	Yes
redundancy procedure MSTP	Yes
Parallel Redundancy Protocol (PRP)/operation in the PRP-network Parallel Redundancy Protocol (PRP)/Parallel Redundant Network Protocol (PRP)/Parall	Yes
 Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA) 	No
passive listening	Yes
protocol / is supported • LACP	Yes
system modification during operation	160
product function / configuration in RUN via CiR/H-CiR	Yes
product functions / security	
product function / security	
• IEEE 802.1x (radius)	Yes
RADIUS client	Yes
broadcast/multicast/unicast limiter	Yes
broadcast blocking	Yes
protocol / is supported	
• SSH	Yes
• SSL	Yes
product functions / time	

s SICL OCK support NTP - client Yes SNTP SNTP SNTP Yes SNTP SNTP Yes SNTP SNTP Yes SNTP		
NTP	•	
SNTP clerk Protocol / is supported NTP SNTP SITP SITP SITP SITE E 1588 profile default Pes Standards, specifications, approvals Certificate of suitability CE marking Site of interference emission Final for immunity to EMC Fi	SICLOCK support	Yes
protocol //s supported • NTP • EIEE 1588 profile default **TeE 1588 profile default **TeE 1588 profile default • NEW Yes • Regulation, approvals certificate of suitability • Regulation / Compliance Mark (RCM) • Regulation / Compliance Mark (RCM) • Regulation / Compliance Mark (RCM) • Tee 1588 profile default **TeE 1589 profi	NTP-client	Yes
NTP NTP NTP NEE 1588 profile default Yes Litted ards, specifications, approvals certificate of subability CE marking Nee Regulatory Compliance Mark (RCM) Yes North Cited interference emission North Cited interferen	SNTP client	Yes
• SNTP	protocol / is supported	
I EEE 1588 profile default Standards, spicifications, spopovals Certificate of suitability OE marking I Ves I Regulatory Compliance Mark (RCM) Fer Gegulatory Compliance Mark (RC	• NTP	Yes
certificate of suitability	• SNTP	Yes
certificate of suitability	IEEE 1588 profile default	Yes
CE marking UKCA marking Ves Regulatory Compliance Mark (RCM) Ves standard For EMC Interference emission For artery / from CSA and UL For safety / from CSA and	standards, specifications, approvals	
Regulatory Compliance Mark (RCM) Standard of or EMC interference emission of immunity to EMC of sately / from CSA and UL UL 62988-1 E115352, CSA C22.2 No. 62988-1 standards, specifications, approvals / other certificate of suitability ROHS conformity	certificate of suitability	
Regulatory Compliance Mark (RCM) Islandard In or EMC Interference emission Find immunity to EMC In safety / from CSA and UL Islandards, specifications, approvals / other Certificate of suitability RoHS conformity RoHS conformity RoHS conformity RoHS conformity Federance temperature / for MTBF determination Roman of the second of the seco	CE marking	Yes
standard of or EMC interference emission of or safety / from CSA and UL EN 61000-6-2 UL 6288-1 E115352, CSA C22.2 No. 62368-1 Standards, specifications, approvals / other certificate of suitability or RoHS conformity Yes product functions / general MTBF 52.a reference temperature / for MTBF determination reference code occording to IEC 81346-2 occording to IEC 81346-2 occording to IEC 81346-2 occording to IEC 81346-2:2019 KFE Varranty period for owebsite: Selection guide for cables and connectors to web page: 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: Industry Online Support to website: Industry Online Support thiss://www.siemens.com/sstatioud thiss:/	UKCA marking	Yes
• for EMC Interference emission • for immunity to EMC • for safety from CSA and UL • Standards, specifications, approvals / other certificate of suitability • RoHS conformity • RoHS conformit	Regulatory Compliance Mark (RCM)	Yes
for immunity to EMC for safety / from CSA and UL standards, specifications, approvals / other Certificate of suitability RoHS conformity Pes product functions / general MTBF		
for immunity to EMC for safety / from CSA and UL standards, specifications, approvals / other Certificate of suitability RoHS conformity Pes product functions / general MTBF	for EMC interference emission	EN 61000-6-4 (Class A)
* for safety / from CSA and UL standards, specifications, approvals / other certificate of suitability * RoHS conformity * S2 a reference temperature / for MTBF determination * 40 °C reference code * according to IEC 81346-2 * b to website. Selection guide for cables and connectors * to web bate. Selection guide for cables and connectors * to website. Industrial communication * to website. Indu		
estandards, specifications, approvals / other certificate of suitability ROHS Conformity Product functions / general MTBF 52 a reference temperature / for MTBF determination reference code according to IEC 81346-2 according to IEC 81346-2:2019 KFE Warranty period 5 a product function / is supported / identification link ot to website: Selection guide for cables and connectors to web page: Selection and TIA Selection Tool to website: Industrial communication to web page: SiePortal to website: Industrial communication to web page: SiePortal to website: Industrial communication thips://www.siemens.com/simalic.net https://www.siemens.com/simalic.net https://www.siemens.com/simalic.net https://www.siemens.com/cax to website: Industrial cybersecurity conscious thips://www.siemens.com/cax to website: Industrial cybersecurity conscious security information Siemens provides products and solutions with industrial cybersecurity conditions 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 wantein — a holistic, state-of-the-art industrial cybersecurity conditions do networks against cyber threats, it is necessary to implement — and continuously wanteins and networks against cyber threats, it is necessary to implement — and continuously wanteins and networks against cyber threats, it is necessary and only when appropriate security measures from the interest if and to the extent such a connection	•	
certificate of suitability ROHS conformity Product functions / general MTBF 52 a reference temperature / for MTBF determination reference code - according to IEC 81346-2 - b according to IEC 81346-2 - according to IEC 81346-2 - b according to IEC 81346-2 - according to IEC 81346-2 - b according to IEC 81346-2 - according to IEC 81346-2 - b accordinate to IEC 81346-8 - b accordinate to	•	OL 02300-1 L 113332, OOA 022.2 No. 02300-1
Product functions / general ### TEF ### Teference temperature / for MTBF determination ### Teference temperature / for MTBF determination ### Teference temperature / for MTBF determination ### Teference code ### according to IEC 81346-2 ### according to IEC 81346-2 ### Teference code ### Teferenc		
mTBF	•	Voc
Interestance temperature / for MTBF determination 40 °C reference code		res
reference code a according to IEC 81346-2 a according to IEC 81346-2:2019 Warranty period product function / is supported / identification link (**Test according to IEC 81346-2:2019 Warranty period product function / is supported / identification link (**Test according to IEC 81346-2:2019 Were internet link (**Test according to IEC 81346-2:2019 Were internet link (**Test according to IEC 81346-2:2019 Internet link Internet link Internet link Internet link Int		
reference code a according to IEC 81346-2 a according to IEC 81346-2:2019 Warranty period 5 a product function / is supported / identification link Yes; acc. to IEC 61406-1:2022 further link 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: CAx-Download-Manager • to website: Industry Online Support • to metalion • Siemens provides products and solutions with industrial cybersecurity information Security information Siemens provides products and solutions with industrial cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access ruly concept. Siemens products 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 networks. Such systems, machines and networks against cyber functions that support the secure operation of 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. Customers are responsible for preventing unauthorized access their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet 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 measure		
according to IEC 81346-2 according to IEC 81346-2:2019 KFE Warranty period product function / is supported / identification link Yes; acc. to IEC 61406-1:2022 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 to website: Industry Online Support thtps://www.siemens.com/simpatic-net https://www.siemens.com/biddb https://www.siemens.com/biddb https://www.siemens.com/cax https://www.siemens.com/cax security information Security information Security information Seews accurate of the communication 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 cybersecy ocnep. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized accomponents should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures that may be implemented, please visit www.siemens.com/cybersecurity measures products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates 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. (V4.7)	·	40 °C
warranty period 5 a product function / is supported / identification link Yes; acc. to IEC 61406-1;2022 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: 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 against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecy to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecy to make the work of the plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized accomponents should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures are applied as soon as they are available and that the latest product updates, subscribe to the Siemens industrial Cybersecurity reasures are applied as soon as they are available and that the latest product updates may increase customer's exponsible for between the place. For additional information on industrial cybersecurity measures are applied as soon as they are available and that the latest product updates are applied as soon as they are available and that the latest product updates are applied as soon as they are available and that the latest product updates are applied as soon as they are available and that the l	reference code	
Warranty period 5 a product function / is supported / identification link Yes; acc. to IEC 61406-1:2022 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: Image database • 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. In order to protect plants, systems, anachines 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 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 segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cest-curity-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	according to IEC 81346-2	KF
product function / is supported / identification link 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: Industry Online Support security information Security 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. 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 segmentate on plants, systems, machines and components should only be connected to an enterprise network or the internet if and to the extent	• according to IEC 81346-2:2019	KFE
Internet link intern	Warranty period	5 a
internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web site: Industrial communication • to web site: SiePortal • to website: Industrial communication • to website: Industrial communication • to website: Industry Online gupport • 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 flustrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	product function / is supported / identification link	Yes; acc. to IEC 61406-1:2022
to website: Selection guide for cables and connectors to to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal to website: Industrial communication to website: Image database to website: Image database to website: Industry Online Support 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 holistic, state-of-the-art industrial cybersecurity concept. Siemens provides 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 pleasures (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 measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures to applied as soon as they are available and that the latest product versions are a spelled as soon as they are available and that the latest product versions are applied as soon as they are available and that the latest product versions are a spelled as soon as they are available and that the latest product versions are available and that the latest product version	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 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. In order to protect plants, systems, machines and networks all norder to protect plants, systems, machines and networks 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	internet link	
to website: Industrial communication 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, systemy, 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: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://www.siemens.com/cax to website: Industry Online Support security information security information 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 flustrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-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 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 website: Industrial communication	https://www.siemens.com/simatic-net
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) Approvals / Certificates	to web page: SiePortal	https://sieportal.siemens.com/
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) Approvals / Certificates	to website: Image database	https://www.automation.siemens.com/bilddb
security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (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	-	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 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		https://support.industry.siemens.com
Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	, , , ,	
Approvals / Certificates	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 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
	Approvals / Certificates	
		Industrial Communication







Miscellaneous

PROFINET

last modified: 1/28/2025 🖸