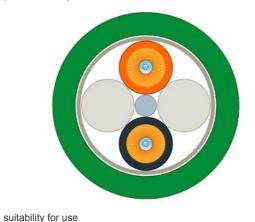
## **SIEMENS**

**Data sheet** 6XV1861-2A

## product type designation product description



## PCF Standard Cable GP

PCF fiber-optic cable with plastic cladding, sold by the meter, unassembled

PCF Standard Cable, (200/230), standard cable splittable, UL approval, without connector, sold by the meter, minimum order quantity 20 m, max. length 2000 m.

suitability for use	Cable for permanent installation indoors and outdoors, UL approval
version of the assembled FO cable	sold by the meter
cable designation	AT-V(ZN)YY 2K 200/230
optical data	
attenuation factor per length	
• at 650 nm / maximum	10 dB/km
• at 660 nm / maximum	10 dB/km
bandwidth length product	
• at 650 nm	17 GHz·m
mechanical data	
number of fibers / per FOC core	1
number of FO cores / per FOC cable	2
version of the FO conductor fiber	Step index fiber 200/230 µm
outer diameter	
<ul> <li>of the optical fibers</li> </ul>	200 μm
<ul> <li>of the optical fiber sheath</li> </ul>	230 μm
of the FOC core sheath	2.2 mm
symmetrical deviation / of the outer diameter of the FOC core sheath	0.1 mm
outer diameter / of the cable	7.2 mm
symmetrical deviation / of the outer diameter of the line	0.5 mm
material	
<ul> <li>of the fiber-optic cable core</li> </ul>	Quartz glass
<ul> <li>of the optical fiber sheath</li> </ul>	Special polymer
<ul> <li>of the FOC core sheath</li> </ul>	PVC
<ul> <li>of the fiber-optic cable sheath</li> </ul>	PVC
of the strain relief	Aramid fibers
color	
• of the FOC core sheath	orange/black
of cable sheath	green
bending radius	
<ul><li>with single bend / minimum permissible</li></ul>	70 mm
with multiple bends / minimum permissible	105 mm
tensile load	
<ul> <li>during installation / short-term</li> </ul>	800 N
during operation / maximum	100 N
short-term shear force per length	500 N/cm
continuous shear force per length	300 N/cm

ambient conditions  arbient temperature  • during potention • during poperation • during storage  • during iteraport  • during iteraport  • during installation  -5 +50 °C  fire behavior  • during misuliation  -5 +50 °C  fire behavior  • during installation  -5 +50 °C  fire behavior  • during installation  -5 +50 °C  fire delension in the storage of	weight per length	45 kg/km
ambient temperature  • Cuiring operation  • Cuiring storage  • Quiring installation  • Cuiring install		40 Ng/MII
during peration     during storage     during transport     during installation     during installation     during installation     dess of burning behaviour / according to EN 13501-6     dess of burning burni		
during storage     during transport     during installation     during installation     during installation     during installation     during installation     during installation     during transport     during behaviour / according to EN 13501-6     desired burning behaviour / according to EN 13501-7     desired burning behaviour / according to EN 13501-7     desired burning burni		40 ±00 °C
during transport     during installation     during installation     description     during installation     description		
- during installation - 5		
fire behavior  class of burning behaviour / according to EN 13501-8  Eca  chemical resistance  • to mineral oil  • to grease • to water  according to EN 13501-8  conditional resistance  • to water  radiological resistance  • hadogen-free • selicon-free  Product component / rodent protection  No  wire length • for PCF FOC / for Industrial Ethernet / maximum • for PCF FOC / for Industrial E		
class of burning behaviour / according to EN 13501-8  Chemical resistance  1 o mineral oil 1 to grease 2 onditional resistance  2 onditional resistance 2 onditional resistance 2 onditional resistance 2 onditional resistance 3 onditional resistance 3 onditional resistance 3 onditional resistance 4 to under resistance 4 onditional resistance 5 onditional resistance 5 onditional resistance 6 onditional resistance 6 onditional resistance 7 onditional resistance		
chemical resistance  • to mineral oil • to grease • to water radiological resistance / to UV radiation radiological resistance / to UV radiation resistant  product features, product functions, product components / general  product omponent / rodent protection No  wire length • for PCF FOC / for Industrial Ethernet / maximum • for PCF FOC / for Industrial Ethernet / maximum • for PCF FOC / with PROFIBUS / maximum  ### 100 m  ### 100		
* to mineral oil     * to grease     * to water  radiological resistance / to UV radiation  resistance  **Resistance  **No  **silicon-free  **Pes  **Poduct component / radent protection  No  wire length  **of PCF FOC / for Industrial Ethernet / maximum  **of PCF FOC / with PROFIBUS / washing / with resistance / visitability  **outhors of witability  **Pes; UL approval: cULus OFN (NEC Article 770, UL 1851) / CSA approval: OFN FT4 (CSA standard C22.2 No. 232)  **Pes / Ves.** UL approval: cULus OFN (NEC Article 770, UL 1851) / CSA approval: OFN FT4 (CSA standard C22.2 No. 232)  **Pes / Ves.** UL approval: with resistance / ves.** Ves.** UL approval: culture of ves.** Ves.** UL approval: ofn ves.** Ves.** Ves.** United ves.** Ves.*		Eca
to grease     to water     to water     conditional resistance     conditional resistance     conditional resistance     resistant  resist		occ to IEC 60911 404 with test oil IDM 002 (occ to ISO 1917) 170 °C 4 h
conditional resistance resistant rediological resistance / to UV radiation resistant  product feature		
radiological resistance / to UV radiation resistant  product features, product functions, product components / general  product feature		
product feature  halogen-free halogen-free halogen-free silicon-free yes product component / rodent protection wire length for PCF FOC / for Industrial Ethernet / maximum for PCF FOC / with PROFIBUS / maximum how for PCF FOC / with PROFIBUS / maximum  for PCF FOC / with PROFIBUS / with		
product feature  • halogen-free • silicon-free • silicon-free • product component / rodent protection No wire length • for PCF FOC / for Industrial Ethernet / maximum • for PCF FOC / with PROF IBUS / maximum  * for PCF FOC / with PROF IBUS / maximum  * for PCF FOC / with PROF IBUS / maximum  * for PCF FOC / with PROF IBUS / maximum  * standards, specifications, approvals  * certificate of suitability • UL approval • RoHS conformity  * Pes; UL approval: cULus OFN (NEC Article 770, UL 1651) / CSA approval: OFN FT4 (CSA standard C22.2 No. 232)  * yes  * reference code • according to IEC 81346-2 • according to IEC 81346-2.2019  * WHA  * further information / internet links  internet link • to web page: SiePortal • to website: Inague database • to website: Industry Online Support  * bittps://support.industry.siemens.com/  * security information / header  * Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to precept plants, systems, machines and networks. In order to precept plants, systems, machines and networks. Such systems, machines and networks such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. First of the top the exercise operation on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/orapirate security measures that may be implemented, please visit or preventing unauthorized access to frain to the exerter such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For plants, systems, machines and networks. Such systems, com/orapirate security measures (e.g. firewalls and/or network segmentation) are in place. For plants, systems, machines an		
No     islicon-free		eneral
Silicon-free     product component / rodent protection     No  wire length	'	
product component / rodent protection  wire length  • for PCF FOC / for Industrial Ethernet / maximum  • for PCF FOC / with PROFIBUS / maximum  standards, specifications, approvals  certificate of suitability  • UL approval  • ROHS conformity  • UL approval:  • ROHS conformity  • WH  • according to IEC 81346-2  • according to IEC 81346-2:  • according to IEC 81346-2:  • to web page: SiePortal  • to web page: SiePortal  • to website: Innage database  • to website: Industry Online Support  security information  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. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement — and continuously maintain — a holistic, 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 against cyber threats, it is necessary to implement — and continuously maintain — a holistic, of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks against cyber eventing unauthorized access to their plants, systems, machines and networks was 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 are applied 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 applied as soon as they are available and the sub	-	
wire length  • for PCF FOC / for Industrial Ethernet / maximum  • for PCF FOC / with PROFIBUS / maximum  100 m  • for PCF FOC / with PROFIBUS / maximum  200 m  standards, specifications, approvals  certificate of suitability  • UL approval  • RoHS conformity  reference code  • according to IEC 81346-2  • according to IEC 81346-2:2019  WHA  further information / internet links  internet link  • to web page: SiePortal  • to website: Industry Online Support  https://sieportal.siemens.com/  • to website: Industry Online Support  security information / header  security information / header  security information / header  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. 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 on element of years against cyber threats, it is necessary to implement—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. ifrewalis and/or 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. ifrewalis and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. ifrewalis and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. ifrewalis and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. ifrewalis and/or networks segmentation) ar		
• for PCF FOC / for Industrial Ethernet / maximum • for PCF FOC / with PROFIBUS / maximum  standards, specifications, approvals  certificate of suitability • UL approval • RoHS conformity  reference code • according to IEC 81346-2 • according to IEC 81346-2.2019  WHA  further information / internet links  internet link • to web page: SiePortal • to website: Image database • to website: Image database • to website: Industry Online Support  security information / header  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 onetworks such systems, nechines and one one such should only be one necessary to implement and such such such systems, nechines and one one one such should only be one necessary to implement and such such such such such such such		No
• for PCF FOC / with PROFIBUS / maximum  standards, specifications, approvals  certificate of suitability  • UL approval  PROHS conformity  reference code  • according to IEC 81346-2  • according to IEC 81346-2  • according to IEC 81346-2  • be web page: SiePortal  • to website: Image database  • to website: Industry Online Support  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 as one		
certificate of suitability  • UL approval  PROHS conformity  Yes: UL approval: cULus OFN (NEC Article 770, UL 1651) / CSA approval: OFN FT4 (CSA standard C22.2 No. 232)  • ROHS conformity  Yes  reference code  • according to IEC 81346-2  • according to IEC 81346-2: WH  further information / Internet links  internet link  • to web page: SiePortal  • to website: Image database  • to website: Industry Online Support  bittps://support.industry.siemens.com/  security information / header  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks under 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 their internet if and to the extent such a connection is necessary and only when appriate 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 (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 (e.g., firewalls and/or network segmentation) are in place are applied as soon as they are available and that the latest product versions are used. Use of product versions have no longer supported, and fallure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens infolutria		
certificate of suitability  • UL approval  Pes: UL approval: cULus OFN (NEC Article 770, UL 1651) / CSA approval: OFN FT4 (CSA standard C22.2 No. 232)  • RoHS conformity  reference code  • according to IEC 81346-2  • MH  • according to IEC 81346-2:2019  WHA  further information / internet links  internet link  • to web page: SiePortal  • to website: Image database  • to website: Image database  • to website: Industry Online Support  security information / header  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 their plants, systems, machines and networks such systems, machines and only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when a propriate security and only be connected to an enterprise network or the internet, 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 have a used. Use of product versions have a used. Use of product versions are a used. Use of product versions are used. Use of product versions are used. Use of product versions are a politic to apply the latest updates may increase outsomer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemen		400 m
Pes; UL approval: cULus OFN (NEC Article 770, UL 1651) / CSA approval: OFN FT4 (CSA standard C22.2 No. 232)  Perference code  According to IEC 81346-2  According to IEC 81346-2: WH  WHA  Further information / internet links  Internet link  No web page: SiePortal  No website: Image database  No website: Image database  No website: Image database  No website: Industry Online Support  Normation / header  Security information / header  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-industry. Siemens' products and solutions undergo continuous develors that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous develors that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous develorent 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 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	standards, specifications, approvals	
ROHS conformity Yes  reference code  according to IEC 81346-2  according to IEC 81346-2:2019 WHA  further information / internet links  internet link  to web page: SlePortal to website: Image database to website: Industry Online Support  security information / header  Security information / header  Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks astate-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) er pladee. For additional information on industrial cybersecurity measures 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	certificate of suitability	
reference code  according to IEC 81346-2  turner link  internet link  to web page: SiePortal  thtps://sieportal.siemens.com/  https://support.industry.siemens.com/  bitus://support.industry.siemens.com/  security information / header  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	UL approval	OFN FT4 (CSA standard C22.2 No. 232)
according to IEC 81346-2  according to IEC 81346-2:2019  WHA  further information / internet links  internet link  to web page: SiePortal  to website: Image database  to website: Industry Online Support  https://support.industry.siemens.com/  https://support.industry.siemens.com/  security information / header  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 onetworks. Such systems, machines and onetworks 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' 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 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	RoHS conformity	Yes
according to IEC 81346-2:2019  further information / internet links  internet link      to web page: SiePortal     https://sieportal.siemens.com/     to website: Image database     https://support.industry.siemens.com/  security information / header  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 RSF Feed under	reference code	
internet link  • to web page: SiePortal • to website: Image database • to website: Industry Online Support  **Security information / header*  **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 onetworks. Such systems, machines and onetworks 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	-	
internet link  • to web page: SiePortal  • to website: Image database  • to website: Industry Online Support  **Security information / header  **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-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		WHA
to web page: SiePortal     to website: Image database     to website: Industry Online Support     https://support.industry.siemens.com/bilddb     https://support.industry.siemens.com  security information / header  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	further information / internet links	
* to website: Image database     * to website: Industry Online Support  **security information / header  **Security information	internet link	
Security information / header  Security information / header  Security information / header  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	to web page: SiePortal	
security information / header  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	to website: Image database	https://www.automation.siemens.com/bilddb
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://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	security information / header	
-T ( · · · · )		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

**General Product Approval** 

Manufacturer Declaration



Declaration of Conformity







other Environment Industrial Communication

Confirmation Confirmation PROFINET

last modified: 6/3/2024 🖸