## **SIEMENS**

Data sheet 6XV1820-5BT10

product type designation
product description

## Fiber optic standard cable

Flexible glass fiber-optic cable, preferred length, preassembled

fiber optic cable (62.5/125), standard cable, splittable, pre-assembled with 4 BFOC connectors, length 100 m.



suitability for use	Cable for installation indoors and outdoors
version of the assembled FO cable	Assembled with four BFOC connectors
cable designation	AT-V(ZN)YY 2X1 G 62,5/125 OM1
wire length	100 m
optical data	
attenuation factor per length	
• at 850 nm / maximum	3 dB/km
• at 1300 nm / maximum	0.8 dB/km
bandwidth length product	
• at 850 nm	300 GHz·m
• at 1300 nm	800 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	Multimode graded-index fiber 62.5/125 μm, OM 1
design of the FOC core	Compact core, diameter 900 µm
design of the fiber-optic cable	Segmentable outer conductor
outer diameter	
<ul> <li>of the optical fibers</li> </ul>	62.5 µm
<ul> <li>of the optical fiber sheath</li> </ul>	125 μm
of the FOC core sheath	3.5 mm
width / of cable sheath	9.8 mm
thickness / of cable sheath	6.3 mm
material	
<ul> <li>of the fiber-optic cable core</li> </ul>	Quartz glass
<ul> <li>of the optical fiber sheath</li> </ul>	Quartz glass
<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 and glass roving
color	
<ul> <li>of the FOC core sheath</li> </ul>	gray
of cable sheath	Black
bending radius	
<ul><li>with single bend / minimum permissible</li></ul>	80 mm
with multiple bends / minimum permissible	80 mm
tensile load	
<ul><li>during installation / short-term</li></ul>	1500 N
<ul> <li>during operation / maximum</li> </ul>	1500 N

that support the secure operation of plants, systems, machines and network 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 responsi for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroin 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update	continuous shear force per length	150 N/cm
ambient temperature  during storage during transport during strange during transport during shallation 5	weight per length	70 kg/km
during storage     during interaport	mbient conditions	
during staraget     during installation     during starting of installation     individual in	ambient temperature	
during transport     during installation     duri	during operation	-40 +85 °C
### during installation ### of commercial resistance ### to mineral oil ### on the resistant ### to mineral oil ###	during storage	-40 +85 °C
### during installation  ### during installati	during transport	-40 +85 °C
chemical resistance  • to mineral oil progresse  not resistant  • to gresse not of the sistance of to UV radiation  radiological resistance of to UV radiation  protection class IP  roduct feature  • halogen-free  • silicon-free  • silicon-free  • silicon-free  • silicon-free  • silicon-free  • resistant  • for glass FOC / for 1008aseFX / for Industrial Ethernet / maximum  • for glass FOC / for 1008aseFX / for Industrial Ethernet / maximum  • for glass FOC / for 1008aseFX / for Industrial Ethernet / maximum  • for glass FOC / for 1000BaseFX / for Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS / maximum  • for glass FOC / with PROFIBUS / maximum  • for glass FOC / with PROFIBUS / maximum  • for glass FOC / with page: siefond in glass of the silicon-free oode  • according to IEC 81346-2 2019  with reference code  • according to IEC 81346-2 2019  with page: siefond aid TIA Selection Tool  • to website: Selection guide for cables and connectors  • to web page: siefond aid TIA Selection Tool  • to website: Industrial communication  • to website: Industrial communication  • to website: Industrial communication  • to website: CAx-Download-Manager  • to website: CAx-Download-Manager  • to website: CAx-Download-Manager  • to website: CAx-Download-Manager  • to website: Industry Online Support  security information / header  security inf		-5 +50 °C
chemical resistance  • to mineral oil  • to grease  not resistant  not resistant  not resistant  not resistant  resistant  resistant  product feature  • halogen-free  • silicon-free  • silic		flame-resistant acc. to IEC 60332-1-2 and IEC 60332-3-22 (Cat. A)
* to grease radiological resistance / to UV radiation protection class IP   P20   P20   P30	chemical resistance	
radiological resistance / to UV radiation resistant protection class IP P20  product feature  • halogen-free •	• to mineral oil	not resistant
radiological resistance / to UV radiation resistant protection class IP P20    P20	• to grease	not resistant
protection class IP  roduct features, product functions, product components / general  roduct feature  • halogen-free  • halogen-free  • slicon-free  product component / rodent protection  wire length  • for glass FOC for 100BaseEX / for Industrial Ethernet / maximum  • for glass FOC for 100BaseSX / for Industrial Ethernet / maximum  • for glass FOC for 100BaseSX / for Industrial Ethernet / maximum  • for glass FOC / for 100BaseSX / for Industrial Ethernet / maximum  • for glass FOC / for 100BaseSX / for Industrial Ethernet / maximum  • for glass FOC / for 100BaseSX / for Industrial Ethernet / maximum  • for glass FOC / for 100BaseSX / for Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS /		resistant
product features   product features   product components / general		
product feature  • halogen-free • silicon-free Product component / rodent protection  wire length • for glass FCC / for 1008aseFX / for industrial Ethernet / maximum • for glass FCC / for 1008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC / for 10008aseEX / for industrial Ethernet / maximum • for glass FCC /	•	
halogen-free     silcon-free     yes      product component / rodent protection  wire length     for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum     for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum     for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum     for glass FOC / for 100BaseFX / for industrial Ethernet / maximum     for glass FOC / for 100BaseFX / for industrial Ethernet / maximum     for glass FOC / with PROFIBUS		···
Silicon-free  Yes  product component / rodent protection  No  No  No  No  No  No  No  No  No	•	No
product component / rodent protection wire length  • for glass FCC / for 1008aseFX / for Industrial Ethernet / maximum • for glass FCC / for 1000BaseSX / for Industrial Ethernet / maximum • for glass FCC / for 1000BaseSX / for Industrial Ethernet / maximum • for glass FCC / with PROFIBUS / w	9	
wire length  • for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum  • for glass FOC / for 1000BaseSX / for Industrial Ethernet / maximum  • for glass FOC / for 1000BaseLX / for Industrial Ethernet / maximum  • for glass FOC / for 1000BaseLX / for Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS / maximum  3000 m  **Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS / maximum  3000 m  **Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS / maximum  3000 m  **Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS / maximum  3000 m  **Industrial Ethernet / maximum  • for glass FOC / with PROFIBUS / maximum  3000 m  **Industrial Ethernet / maximum  4000 m  4000 m		
• for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum		INU
For glass FOC / for 1000BaseSX / for Industrial Ethernet / maximum	• for glass FOC / for 100BaseFX / for Industrial Ethernet /	4000 m
when the properties of suitability RoHS conformity RoHS conformity RoHS conformity RoHS conding to IEC 81346-2 According to IEC 81346-2 According to IEC 81346-2:2019 WHA  wither 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: CAx-Download-Manager to website: CAx-Download-Manager to website: Industry Online Support  Security information / header  Security information  Siemens provides products and solutions with industrial cybersecurity functions constitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and networks. Such systems, machines and removes against and that the latest product utpatates are applied as soon as they are available and that the lat		500 m
certificate of suitability ROHS conformity Yes  Yes  Yes  Yes  According to IEC 81346-2  • according to IEC 81346-2:2019 WHA  urther 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: Ind		1000 m
reference code  according to IEC 81346-2  according to IEC 81346-2  what  internet link  i to website: Selection guide for cables and connectors  to web page: selection aid TIA Selection Tool  to website: Industrial communication  to website: Industri page database  to website: Industry Online Support  thtps://www.aiemens.com/csa/ww/en/view/109766358  https://www.aiemens.com/simatic-net  https://www.aiemens.com/simatic-net  https://www.aiemens.com/csimatic-net  https://www.aiemens.com/csa/ww/en/view/109766358  to website: Industrial cybersecurity  thtps://www.aiemens.com/simatic-net  https://www.aiemens.com/csa/ww/en/view/109766358  https://www.aiemens.com/simatic-net  https://www.aiemens.com/simatic-net  https://www.aiemens.com/csa/wwien/view/109766358  https://www.aiemens.com/simatic-net  https://www.aiemens.com/csa/wwien/view/109766358  https://www.aiemens.com/simatic-net  https://www.aiemens.com/csa/wwien/view/109766358  https://www.aiemens.com/simatic-net  https://www.aiemens.com/simatic-net  https://www.aiemens.com/csa/wwien/view/109766358  https://www.aiemens.com/simatic-net  https://www.aiem	<ul><li>for glass FOC / with PROFIBUS / maximum</li></ul>	3000 m
reference code  according to IEC 81346-2  according to IEC 81346-2:2019  WHA  urther information / internet links  internet link  • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support • to website:	tandards, specifications, approvals	
reference code  according to IEC 81346-2  according to IEC 81346-2:2019  WHA  writer information / internet links  internet link  to website: Selection guide for cables and connectors  to web page: selection aid TIA Selection Tool  to website: Industrial communication  to website: Industrial communication  to website: Image database  to website: Image database  to website: Image database  to website: Industry Online Support  to website: Industry Online Support  https://www.siemens.com/simatic-net  https://www.siemens.com/simatic-net  https://www.siemens.com/cax  https://www.siemens.com/cax  to website: Industry Online Support  security information / header  Security information / header  Security information / header  Siemens provides products and solutions with industrial cybersecurity function 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 ossitute one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect on an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and networks 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 stroe recommends that product varies are as they are available and that the latest product versions are used. Use of product versions that an olonger supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update outsomer's exposure to cyber threats. To stay informed about	certificate of suitability	
according to IEC 81346-2 according to IEC 81346-2:2019 WHA  wither information / internet links internet link  to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Industrial communication to website: Image database to website: Image database to website: Image database to website: Industry Online Support to website: Industry Online Support thitps://www.siemens.com/simatic-net https://www.siemens.com/cax to website: Industry Online Support  Siemens provides products and solutions with industrial cybersecurity function 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 responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cyberaccurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens stro recommends that product pudates are applied as soon as they are available and that the latest product versions are used. Use of product versions that an olonger supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that an olonger supported, and failure to apply the late	<ul> <li>RoHS conformity</li> </ul>	Yes
according to IEC 81346-2:2019  WHA  writher 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 web page: SiePortal to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support thttps://www.automation.siemens.com/bilddb thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://sieportal.siemens.com/cax thttps://sieportal.siemens.com/cax thttps://sieportal.siemens.com/cax thttps://sieportal.siemens.com/cax thttps://sww.automation.siemens.com/bilddb thttps://sww.siemens.com/cax t	reference code	
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: Induser adatabase • to website: CAx-Download-Manager • to website: Industry Online Support • those of the secure operation of plants, systems, machines and networks norder 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. Suemen's products and solutions constitute one element of such a concept. Customers are responsi for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/unetwork segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit  www.siemens.com/csaw  undergo continuous development to make them more secure. Siemens stronger supported, and failure to apply the latest updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that an olonger supported, and failure to apply the latest updat	<ul> <li>according to IEC 81346-2</li> </ul>	WH
internet link  • to website: Selection guide for cables and connectors  • to web page: selection aid TIA Selection Tool  • to website: Industrial communication  • to web page: SiePortal  • to website: Image database  • to website: Industry Online Support  • to website: Industry Support Industry Support  • to website: Industry Support Industry Support  • to website: Industry Support Industry Support  • to	<ul> <li>according to IEC 81346-2:2019</li> </ul>	WHA
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: Image database     to to website: Image database     to to website: Image database     to to website: Industry Online Support     to to website: Industry Online Support     thttps://www.automation.siemens.com/bilddb     https://www.siemens.com/cax     https://www.siemens.com/cax     https://support.industry.siemens.com  Security information / header  Security information  Siemens provides products and solutions with industrial cybersecurity function 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 responsi for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 strong 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update	urther information / internet links	
to web page: selection aid TIA Selection Tool     to website: Industrial communication     to web page: SiePortal     to to website: Image database     to to website: Image database     to to website: Image database     to to website: Industry Online Support     to website: Industry Online Support      to website: Industry Online Support      to website: Industry Online Support      to website: Industry Online Support      security information / header  Security information  Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and network 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 responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one onecessary and only when appropriate security measures (e.g. firewalls and/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 stroor 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update	internet link	
<ul> <li>to website: Industrial communication</li> <li>to web page: SiePortal</li> <li>https://sieportal.siemens.com/</li> <li>to website: Image database</li> <li>https://www.automation.siemens.com/bilddb</li> <li>to website: CAx-Download-Manager</li> <li>https://www.siemens.com/cax</li> <li>to website: Industry Online Support</li> <li>https://support.industry.siemens.com</li> <li>security information / header</li> <li>security information</li> <li>Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and network 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 one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroin 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that an olonger supported, and fail</li></ul>	• to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
<ul> <li>to website: Industrial communication</li> <li>to web page: SiePortal</li> <li>https://sieportal.siemens.com/</li> <li>to website: Image database</li> <li>https://www.automation.siemens.com/bilddb</li> <li>to website: CAx-Download-Manager</li> <li>https://www.siemens.com/cax</li> <li>to website: Industry Online Support</li> <li>https://support.industry.siemens.com</li> <li>security information / header</li> <li>security information</li> <li>Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and network 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 one element of such a concept. Customers are responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroin 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that an olonger supported, and fail</li></ul>	• to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
<ul> <li>to website: Image database</li> <li>to website: CAx-Download-Manager</li> <li>to website: Industry Online Support</li> <li>https://support.industry.siemens.com/cax</li> <li>https://support.industry.siemens.com</li> <li>security information / header</li> <li>Siemens provides products and solutions with industrial cybersecurity function 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 responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroit 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates are updated about product updates.</li> </ul>		https://www.siemens.com/simatic-net
<ul> <li>to website: Image database</li> <li>to website: CAx-Download-Manager</li> <li>to website: Industry Online Support</li> <li>https://support.industry.siemens.com/cax</li> <li>https://support.industry.siemens.com</li> <li>security information / header</li> <li>Siemens provides products and solutions with industrial cybersecurity function 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 responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroit 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update</li> </ul>	• to web page: SiePortal	https://sieportal.siemens.com/
to website: CAx-Download-Manager     to website: Industry Online Support      https://support.industry.siemens.com  Siemens provides products and solutions with industrial cybersecurity function 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 responsifor preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroin 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update updates may increase customer's exposure to cyber threats. To stay informed about product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates are supplied as soon as they are available.		
• to website: Industry Online Support    https://support.industry.siemens.com	•	
Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and network 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 one element of such a concept. Customers are responsi for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroir 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update	3	
Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and network 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 responsi for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connect to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 stroit 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 a no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update	,	- International Control of the Contr
	security information	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)	namovala / Cardificados	napo.nwww.oremeno.com/cett. (V4.7)



Declaration of Conformity





Manufacturer Declaration



General Product Approval

Marine / Shipping

other

Environment





Confirmation

Confirmation

last modified:

8/9/2024