## **SIEMENS**

Data sheet 6XV1820-5BH50

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 5  $\mbox{m}.$ 



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	5 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
nechanical 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
<ul> <li>of the FOC core sheath</li> </ul>	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

mobilent conditions ambient temperature  • outring operation  • during storage  • during stations  • to mineral oil  • to grease  reddocpical resistance  • to mineral oil  • to grease  reddocpical resistance  • to mineral oil  • to grease  reddocpical resistance / to UV radiation  resistant  reported feature  • hor glass FOC / for 1008aeFX / for Industrial Ethernet / maximum  • for glass FOC / for 1008aeFX / for Industrial Ethernet / maximum  • for glass FOC / for 1008aeFX / for Industrial Ethernet / maximum  • for glass FOC / for the RPGIBLS / maximum  standards, specifications, approvate  conflicted of suitability  • Act / Scondmanty  • Red / Scondmanty  • India / Scondmanty  • Red / Scondmanty	continuous shear force per length	150 N/cm	
ambient temperature  • during operation • during storage • during ministration • during initialization • fire behavior • during initialization • fire behavior • finame-resistant acu, to IEC 80332-1-2 and IEC 80332-3-22 (Cat. A)  Chemical resistance • for initial resistance • for present initialization • for grease radiological resistance • for grease  • for grease • for for for grease  • for grease • for for for grease • for for grease • for grease • for for for grease • for for for grease • for grease • for for for grease • for for for grease • for grease • for for for grease • for for grease • for for for grease • for grease • for for for grease • for for for grease • for grease • for for for grease • for grease	weight per length	70 kg/km	
eduring stroage eduring transport during istrasport during istrasp	ambient conditions		
eduring stroage eduring transport during istrasport during istrasp	ambient temperature		
Curring storage  Ouring trasport  Our diseases  Our diseases  Our diseases  Our diseases  Our diseases  Ouring trasport  Our diseases  Ouring trasport  Our diseases  Our diseases  Ouring trasport  Our diseases  Ouring trasport  Our diseases  Our diseases  Ouring trasport  Ouring trasport  Our diseases  Our diseases  Ouring trasport  Ouring trasport  Ouring trasport  Our diseases  Ouring trasport  Our diseases  Ouring trasport  Ouring trasport  Ouring trasport  Our diseases  Our diseases  Ouring trasport  Ouring trasport  Ouring trasport  Ouring trasport  Ouring trasport  Our diseases  Our diseases  Ouring trasport  Ouring tras	•	-40 +85 °C	
eduring transport during installation fire behavior for command the process of the process			
- during installation - 5 +50 °C fire behavior - 6 to mineral cil - on rineral cil - on			
fire behavior  Chemical resistance  • to mineral oil  • to grease  • to mineral oil  • to grease  challogical resistance / to UV radiation  protection class IP  product features, product functions, product components / general  product features  • halogen-free  • halogen-free  • halogen-free  • product registant  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for 100BaseFX / for industrial Ethernet / maximum  • for glass FC/ for the formation of plass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum  • for glass FC/ for industrial Ethernet / maximum			
chemical resistance  • to mineral oil  • to grease  radiological resistant  rotrection class IP  product feature  • halogen-free  • silicon-free  product component / rodent protection  No  vive length  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial Ethernet / maximum  • for glass FCC / for 100BaseFX / for industrial E			
to mineral oil		name resistant des. to the edest if a did the edest of the (edit. 7)	
e to grease radiological resistance / to UV radiation protection class IP product features, product functions, product components / general product feature		not resistant	
resistant protection class IP  product features product functions, product components / general  product feature  • halogen-free • halogen-free • silicon-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 / 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 / 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 / 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 / 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 / for 100BaseFX / for industrial Ethernet / maximum • for glass FOC / for 100BaseFX / for industrial Ethernet / ma			
protection class IP product features, product functions, product components / general product feature  • halogen-free • silicon-free • yes product component / rodent protection • No 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 / for 100BaseLX / for industrial Ethernet / maximum • for glass FOC / with PROFIBUS / maximum • for glass FOC / with PROFIBUS / maximum • standards, specifications, approvals certificate of suitability • RoHS conformity • Yes reference code • according to IEC 81346-2-2019  WH  further information / Internet tints  Internet link • to website: Industry Online Support  security information / header  security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation or 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, 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, 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, and solutions occasitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks against one and that the plants are products and solutions occasions and occupance and to such as a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and net			
product features, product functions, product components / general product feature			
product feature  halogen-free  halogen-free  silicon-free  yes  product component / rodent protection  No  wire length  of rogiass FOC / for 1008aseFX / for industrial Ethernet / maximum  of rogiass FOC / for 1008aseSX / for Industrial Ethernet / maximum  of rogiass FOC / for 1008aseSX / for Industrial Ethernet / maximum  of rogiass FOC / for 1008aseSX / for Industrial Ethernet / maximum  of rogiass FOC / with PROFIBUS / maximum  standards, specifications, approvals  certificate of suitability  RoHS conformity  Yes  reference code  according to IEC 81346-2  with  to web page: SiePortal  to website: Industry Online Support  https://www.automation.siemens.com/ https://www.automation.siemens.com/ bhttps://www.automation.siemens.com/ 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 a plants cyber threats, it is necessary to implement – and continuously maintain – a holistic, site-of-the-art industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks in order to protect plants, systems, machines and networks in order to protect plants, systems, machines and components should only be connected to an enterprise network or the industrial cybersecurity oncept cyber threats, it is necessary to implement – and continuously maintain – a holistic, site-of-the-art industrial cybersecurity oncept cybers of threats in the site of the decrease of the plants products and components should only be connected to an enterprise network or the internet if and to make them more secure. Secures should not have a proportial to the product versions are used Love of connected to an enterprise network or the internet if and to internet industrial cybersecurity onces. Semens shou	<u> </u>		
Approvals / Certificates   No	· · · · · · · · · · · · · · · · · · ·	et al	
Silicon-free  product component / rodent protection  No  No  Wrie length  • for glass FOC / for 1000BaseFX / for Industrial Eithernet / maximum  • for glass FOC / for 1000BaseSX / for Industrial Eithernet / maximum  • for glass FOC / for 1000BaseSX / for Industrial Eithernet / maximum  • for glass FOC / for 1000BaseLX / for Industrial Eithernet / maximum  • for glass FOC / with PROFIBUS / maximum  standards , specifications , approvals  certificate of suitability  • RoHS conformity  • RoHS conformity  • 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: Industry Online Support  security information / header  security information / header  Security information / header  Security information / header  Silemens 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 ontinuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens provides 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 and only when appropriate security measures (e.g. firewalls and/or networks. Such systems, machines and connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or networks. Such systems, machines and connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or networks. Such systems, machines and connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropri	·	Na	
product component / rodent protection  wire length  • for glass FOC / for 1008aseFX / 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 / with PROFIBUS / maximum  * for glass FOC / with PROFIBUS / maximum  * for glass FOC / with PROFIBUS / maximum  * for glass FOC / with PROFIBUS / maximum  * standards, specifications, approvals  certificate of suitability  • RoHS conformity  • RoHS conformity  * reference code  • according to IEC 81346-2  • according to IEC 81346-2  • wHA  * to web page: SiePortal  • to website: Image database  • to website: Image database  • to towelpage: SiePortal  • 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 and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks and solutions with industrial cybersecurity concept. Siemens products and solutions or protect plants, systems, machines and networks signate or plants and protect plants signate or plants are appropriate security plants and networ			
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  standards, specifications, approvals  certificate of suitability  • RoHS conformity  • RoHS conformity  Yes  reference code  • according to IEC 81346-2 • with a conformity  • to web page: SiePortal • to website: Image database • to website: Inhabity / with industrial cybersecurity information / internation / hader  Security information / hader  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 aliant or protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks aliant or protect plants, systems, machines and networks. Such systems, machines and networks aliant or networks. Such systems, machines and networks against cyber threats, it is necessary of miplement—and continuously maintain—a holistic, state-of-the-ari industrial cybersecurity one connection is necessary and only when apoptate security measures the responsible for preventing unauthorized access to their plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary and only when apoptate security measures the file of the extent such a connect			
* for glass FOC / for 1000BaseFX / 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 / with PROFIBUS / maximum     3000 m  **standards, specifications, approvals**  certificate of suitability     * RoHS conformity     * RoHS conformity     * reference code     * according to IEC 81346-2     * according to IEC 81346-2.2019     * WHA  **Turther information / internet links**  internet link     * to web page: SiePortal     * to website: Industry Online Support  security information / header  **security		INO	
maximum • for glass FOC / for 1000BaseLX / for Industrial Ethernet / maximum • for glass FOC / with PROFIBUS / maximum 3000 m  standards, specifications, approvals  certificate of suitability • RoHS conformity • According to IEC 81346-2 • 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://www.automation.siemens.com/  https://support.industry.siemens.com  security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Security concept. Securi	• for glass FOC / for 100BaseFX / for Industrial Ethernet /	4000 m	
maximum  • for glass FOC / with PROFIBUS / maximum  standards, specifications, approvals  certificate of suitability  • 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: Imdustry 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 against cyber threats, it is necessary to implement — and continuously maintain — a holistic, state-of-the-art industrial cybersecurity concept. Siemens provides and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access their plants, systems, machines and networks adjants 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 confinuous development for note 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)		500 m	
certificate of suitability  • RoHS conformity  reference code  • according to IEC 81346-2  • 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  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, anachines and networks in order to protect plants, systems, anachines and networks sin order to protect plants, systems, machines and networks solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one tworks. Such systems, machines and one tworks and networks. Such systems, machines and one provides to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are inplemented, 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 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 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.	. •	1000 m	
certificate of suitability  • 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: 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. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implemented 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 plemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product update, read and that the latest product versions are used. Use of product versions hat are no longer supported, and faith at product updates 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)	<ul> <li>for glass FOC / with PROFIBUS / maximum</li> </ul>	3000 m	
RoHS conformity  Perence 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: 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 ostitute 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 underly and only when propriate 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 faller to paply the latest updates may increase outsomer'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)	standards, specifications, approvals		
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 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. firevalls and/or network segmentation) are in place. For additional information on industrial cybersecurity 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 faillure 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	certificate of suitability		
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 / header  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 eybersecurity 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 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 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	RoHS conformity	Yes	
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  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 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)	reference code		
internet link  • to web page: SiePortal  • 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 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 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)	according to IEC 81346-2	WH	
internet link  • to web page: SiePortal  • to website: Image database  • to website: Industry Online Support  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 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	<ul> <li>according to IEC 81346-2:2019</li> </ul>	WHA	
to web page: SiePortal	further information / internet links		
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 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		
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 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/	
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 against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-fite-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 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 latest 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: Image database	https://www.automation.siemens.com/bilddb	
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 https://www.siemens.com/cert. (V4.7)  Approvals / Certificates	3		
Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	security information / header		
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	
	Annroyals / Certificates		

General Floduct Ap



Declaration of Conformity





Manufacturer Declaration



General Product Approval

Marine / Shipping

other

Environment





Confirmation

Confirmation

last modified:

6/3/2024