SIEMENS

Data sheet 6XV1820-5BT13

product type designation
product description

Fiber optic standard cable

Cable for installation indeers and outdeers

Flexible glass fiber-optic cable, preferred length, preassembled

fiber optic cable (62.5/125), standard cable, splittable, pre-assembled with 4 BFOC connectors, length 130 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	130 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	
 of the optical fibers 	62.5 μm
 of the optical fiber sheath 	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	
 of the fiber-optic cable core 	Quartz glass
 of the optical fiber sheath 	Quartz glass
 of the FOC core sheath 	PVC
 of the fiber-optic cable sheath 	PVC
of the strain relief	Aramid fibers and glass roving
color	
 of the FOC core sheath 	gray
of cable sheath	Black
bending radius	
with single bend / minimum permissible	80 mm
with multiple bends / minimum permissible	80 mm
tensile load	
 during installation / short-term 	1500 N
during operation / maximum	1500 N

continuous shear force per length 70 kg/km ambient temperature - during operation - during storage - during statilation - during stati		
ambient temperature • during peration • during storage • during transport • during transport • during transport • during installation • 5 +50 °C • during installation • 5 mineral oil • to grease radiological resistance / to UV radiation resistant resist	continuous shear force per length	150 N/cm
ambient temperature • Juring operation • Juring storage • during storage • Juring stratage • Juring str	weight per length	70 kg/km
during peration during strape during transport during installation during part of the during installation during installation during part of the during installation during part of the during installation in	ambient conditions	
during storage during transport during installation s	ambient temperature	
during transport during traillation fire behavior fire behavior fire behavior fire resistant acc. to IEC 00332-1-2 and IEC 60332-3-22 (Cat. A) chemical resistance in or resistant in or resista	during operation	-40 +85 °C
- during installation - 5+50 °C fire behavior - 6+50 °C - 6+	during storage	-40 +85 °C
fire behavior chemical resistance	during transport	-40 +85 °C
chemical resistance	during installation	-5 +50 °C
to mineral oil	fire behavior	flame-resistant acc. to IEC 60332-1-2 and IEC 60332-3-22 (Cat. A)
• to grease radiological resistance / to UV radiation resistant re	chemical resistance	
radiological resistance / to UV radiation protection class IP IP20 product feature • halogen-free • halogen-free • halogen-free • halogen-free • halogen-free • halogen-free • silicon-free product component / rodent protection No wire 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 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / maximum • for glass FCC / for 100BaseSX / for industrial Ethernet / for product version structure / for product version structure / for preventing unatural read continuously maximum - a holsite, solutions on the security information or industrial repetitive for product version structure on element of such a conceton is necessary and only when appropriate security measures that may be implemented, please visit undet for product versions that are no	• to mineral oil	not resistant
product features, product functions, product components / general product feature • halogen-free • silicon-free • silicon-free • silicon-free • silicon-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 / silicon-filicon industrial Ethernet / ma	• to grease	not resistant
product features, product functions, product components / general product feature	radiological resistance / to UV radiation	resistant
product feature • halogen-free • silicon-free • silicon-free • silicon-free • product component / rodent protection wrice 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 100BaseLX / for Industrial Ethernet / maximum • for glass FOC / with PROFIBUS	protection class IP	IP20
* silicon-free * yes * product component / rodent protection * wire length * 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 * so pedications, approvals * entire continuation / specifications, approvals * entire continuation / spe	product features, product functions, product components / gene	eral
* silicon-free product component / rodent protection No wire length * of rglass FOC / for 100BaseFX / for Industrial Ethernet / maximum * of rglass FOC / for 1000BaseSX / for Industrial Ethernet / maximum * of rglass FOC / for 1000BaseSX / for Industrial Ethernet / maximum * of rglass FOC / for 1000BaseLX / for Industrial Ethernet / maximum * of rglass FOC / with PROFIBUS / wi	product feature	
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 1000BaseSX / for Industrial Ethernet / maximum • for glass FOC / for 1000BaseLX / for Industrial Ethernet / maximum • for glass FOC / with PROFIBUS / w	halogen-free	No
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 standards, specifications, approvals certificate of suitability • RoHS conformity • ROHS conformity • according to IEC 81346-2 • according to IEC 81346-2 • according to IEC 81346-2 • to web page: SiePortal • to web page: SiePortal • to web page: SiePortal • to website: Industry Online Support https://www.automation.siemens.com/ https://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, 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 an achieves and networks. Such systems, machines and networks such systems, machines and intervorks. Such systems, machines and intervorks 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 an achieve for preventing unauthorized access to their plants, systems, machines and networks such as 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 continuo	• silicon-free	Yes
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 standards, specifications, approvals certificate of suitability • RoHS conformity • ROHS conformity ves reference code • according to IEC 81346-2 • wHA further information / Internet link • to web page: SiePortal • to web page: SiePortal • to website: Industry Online Support https://www.automation.siemens.com/ bittos://support.industry.siemens.com security information / heador securi	product component / rodent protection	No
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 3000 m standards, specifications, approvals certificate of suitability • RoHS conformity Yes reference code • according to IEC 81346-2 • wH • according to IEC 81346-2 • WH further information / internet links internet link • to website: Industry Online Support • to website: Industry Online Support https://support.industry.siemens.com/ bluss//swww.automation.siemens.com/ bluss//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. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. Such systems, machines and onetworks. Such systems, machines and onetworks. Such systems, machines and onetworks season when products and solutions constitute one element of an other concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks season when product versions and entworks are seponsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks are seponsible for preventing unauthorized access to their plants, systems, machines and networks segments and only when appropriate security measures (e.g. firewalis and/or network segmentation) are in place. For additional information in necessary and only when appropriate security measures (e.g. firewalis and/or	wire length	
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 Yes reference code • according to IEC 81346-2 • according to IEC 81346-2 • wWHA further information / internet links internet link • to web page: SiePortal • to website: Industry Online Support bitos://sieportal.siemens.com/ • to website: Industry Online Support security information / header securit		4000 m
maximum • for glass FOC / with PROFIBUS / maximum standards, specifications, approvals certificate of suitability • RoHS conformity Yes reference code • according to IEC 81346-22 • according to IEC 81346-22019 WHA further information / internet links internet link • to web page: SiePortal • to website: Image database • to website: Image database • to website: Industry Online Support https://swww.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. 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 nomponents 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. 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. (v4.7.7)		500 m
certificate of suitability • RoHS conformity reference code • according to IEC 81346-2 • according to IEC 81346-2 • macroding to IEC 81346-2 • according to IEC 81346-2:2019 WHA further information / internet links • to web page: SiePortal • to website: Image database • 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. Customers are responsible for preventing unauthorized access to 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 appropriates eccurity measures (e.g. firewalls and/or network security 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)	. The state of the	1000 m
certificate of suitability ROHS conformity Pes reference code according to IEC 81346-2 according to IEC 81346-2:2019 WHA further information / internet links internet link to web page: SiePortal tittps://sieportal.siemens.com/ to website: linage database to website: linage database to website: lindustry 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 networks or a 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 and only when a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures that 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 may increase outstomer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens literate to apply the latest updates may increase outstomer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens to the Siemens and components should and the latest products and solutions undergo continuous de	for glass FOC / with PROFIBUS / maximum	3000 m
RoHS conformity reference code according to IEC 81346-2 twH according to IEC 81346-2:2019 WHA further information / internet links internet link to web page: SiePortal twtps://sieportal.siemens.com/ 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-fihe-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 connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network 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 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.	standards, specifications, approvals	
reference code according to IEC 81346-2 what ruther 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 Slemens 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. Slemens' 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 when appropriate security 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 had 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)	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 titps://sieportal.siemens.com/ 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 one networks. Such systems, machines are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one plants 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 in 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 updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	RoHS conformity	Yes
according to IEC 81346-2:2019 WHA further information / internet links internet link to web page: SiePortal titps://sieportal.siemens.com/ 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 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 Sichers 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 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 a 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 a concept. Siemens' product and networks sugher 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 later 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 **Mitps://sieportal.siemens.com/ **Intips://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 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)	according to IEC 81346-2:2019	WHA
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 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 https://www.siemens.com/cet. (V4.7)	further information / internet links	
to website: Image database to website: Industry Online Support https://support.industry.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. 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)	internet link	
** 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. Slemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	• to web page: SiePortal	https://sieportal.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 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)	• 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://www.siemens.com/cert. (V4.7)	• to website: Industry Online Support	https://support.industry.siemens.com
that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks 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		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



Declaration of Conformity









Marine / Shipping

other

Environment



Confirmation

Confirmation

last modified:

6/3/2024