SIEMENS

Data sheet

6XV1820-5BN70

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 70 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	70 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

weight per length 70 kg/km ambient excertations	continuous shear force per length	150 N/cm
ambient temperature		70 kg/km
ambient temperature • during storage • during		
• during persplane 40		
 40 - 48 °C 40 - 40 - 48 °C 40 - 40 °C 40 °C 40		-40 +85 °C
- during installation - during inst		
• during installation -5+50 °C fire behavior finam-resistance to EC 60332-1-2 and EC 60332-3-22 (Cat. A) • lo nineral ol not resistant • lo nineral ol not resistant • lo nineral ol not resistant redictionas IP IP20 product features resistant redictionas IP IP20 product features No • lalogon free No • lalogon free No • landgon free No • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No 0000 m • for glass FCC / for 1000BaseSX / for Industrial Ethernet / No No • fore glass FCC / for 1000BaseSX / for Industrial Ethernet		
free behavior flame-resistant acc. to IEC 60332-1-2 and IEC 60332-3-22 (Cat. A) chemical resistance not resistant i to minarai all not resistant adlocgical resistance / to UV radiation resistant product features, product functions, product components / general IP20 product features, product functions, product components / general No adlogen/refe No		
chemical resistance i on interal of i on interal i on one interal i on one interal i on one interal i on one interal i on interal i on interal i on interal i on one one one one one one one one one		flame-resistant acc. to IEC 60332-1-2 and IEC 60332-3-22 (Cat. A)
• log gresse not resistant radiological resistance / to UV radiation resistant product floatures, product functions, product components / general P20 product floatures, product functions, product components / general No • alaigon-free No • alaigon-free Yes • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / we		
• log gresse not resistant radiological resistance / to UV radiation resistant product floatures, product functions, product components / general P20 product floatures, product functions, product components / general No • alaigon-free No • alaigon-free Yes • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / for 100BaseSX / for Industrial Ethernet / So0 m • for glass FOC / we		not resistant
radiological resistance / to UV radiation resistant resistant protection dass IP resistance / to UV radiation		
product failures, product functions, product components / general product failures, product failures, product failures i halogen-free Product failures i halogen-free Product failures i failures Product failures		resistant
product feature No • halogen/free No • silicon-free Yes product component / rodent protection No • for glass FCC / for 100BaseFX / for Industrial Ethernet / maximum 4000 m • for glass FCC / for 100BaseFX / for Industrial Ethernet / maximum 500 m • for glass FCC / for 100BaseLX / for Industrial Ethernet / maximum 500 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for there information / informat links • internet link • • to website: Industrial Communication • • to website: Industrind Communication		IP20
product feature No • halogen/free No • silicon-free Yes product component / rodent protection No • for glass FCC / for 100BaseFX / for Industrial Ethernet / maximum 4000 m • for glass FCC / for 100BaseFX / for Industrial Ethernet / maximum 500 m • for glass FCC / for 100BaseLX / for Industrial Ethernet / maximum 500 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for glass FCC / with PROFIBUS / maximum 3000 m • for there information / informat links • internet link • • to website: Industrial Communication • • to website: Industrind Communication	product features, product functions, product components / gene	eral
• silicon-free Yes product component / rodent protection No • for glass FOC / for 1008aseFX / for industrial Ethernet / maximum 4000 m • for glass FOC / for 1000BaseSX / for industrial Ethernet / maximum 500 m • for glass FOC / for 1000BaseSX / for industrial Ethernet / maximum 500 m • for glass FOC / for 1000BaseSX / for industrial Ethernet / maximum 3000 m • for glass FOC / with PROFIBUS / maximum 3000 m standards, specifications, approvals - certificate of suitability Yes • RoHS conformity Yes reference code - • according to IEC 81346-22 WH • to website: Selection guide for cables and connectors https://www.siemens.com/sc/sw/weiv/sw/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/weiv/sw/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 <		
• silicon-free Yes product component / rodent protection No • for glass FOC / for 1008aseFX / for industrial Ethernet / maximum 4000 m • for glass FOC / for 1000BaseSX / for industrial Ethernet / maximum 500 m • for glass FOC / for 1000BaseSX / for industrial Ethernet / maximum 500 m • for glass FOC / for 1000BaseSX / for industrial Ethernet / maximum 3000 m • for glass FOC / with PROFIBUS / maximum 3000 m standards, specifications, approvals - certificate of suitability Yes • RoHS conformity Yes reference code - • according to IEC 81346-22 WH • to website: Selection guide for cables and connectors https://www.siemens.com/sc/sw/weiv/sw/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/weiv/sw/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 • to website: Industrial communication https://www.siemens.com/sc/sw/enview/109768358 <	halogen-free	No
product component / rodent protection No wire length 4000 m • for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum 4000 m • for glass FOC / for 100BaseLX / for Industrial Ethernet / maximum 500 m • for glass FOC / for 100BaseLX / for Industrial Ethernet / maximum 1000 m • for glass FOC / with PROFIBUS / maximum 3000 m • tor glass FOC / with PROFIBUS / maximum 3000 m • tor glass FOC / with PROFIBUS / maximum 3000 m • tandards, specifications, approvals Certificate of suitability • RoHS conformity Yes reference code • according to IEC 81346-2 • to website: Selection guide for cables and connectors https://support.industry.siemens.com//scivw/enview/109766358 • to website: Selection quide for cables and connectors https://support.industry.siemens.com//scivw/enview/109766358 • to website: Industrial communication https://support.industry.siemens.com//scivw/enview/109766358 • to website: Industrial communication https://support.industry.siemens.com//scivw/enview/109766358 • to website: Industrial communication https://www.siemens.com//scivw/enview/109766358 • to website: Industrial communication https://www.siemens.com//scivw/enview/	-	
wire length for glass FOC / for 100BaseFX / for Industrial Ethernet / maximum for glass FOC / for 100BaseSX / 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 / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC / with PROFIBUS / with a for glass FOC /		
maximum • for glass FOC / for 1000BaseLX / for Industrial Ethernet // maximum 1000 m • for glass FOC / with PROFIBUS / maximum 3000 m standards, specifications, approvals Certificate of suitability • RoHS conformity Yes • according to IEC 81346-2:2019 WH • according to IEC 81346-2:2019 WHA futner Internet link • to website: Selection guide for cables and connectors https://support.industry.siemens.com/tsto/wu/10/9766358 • to website: Selection guide for cables and connectors https://support.industry.siemens.com/tsto/ud • to website: Industrial communication https://www.siemens.com/tsto/ud • to website: Industrial communication https://www.siemens.com/simatic.net • to website: Industrial communication https://www.siemens.com/simatic.net • to website: Industrial orgeneration in the support https://support.industry.siemens.com/simatic.net • to website: Industrial orgeneration in the support https://support.industry.siemens.com/simatic.net security information https://support.industry.siemens.com/simatic.net https://support.industry.siemens.com/simatic.net security information ntds:/support.industry.siemens.com/simatic.net https://support.industry.siemens.com/simatic.net	• for glass FOC / for 100BaseFX / for Industrial Ethernet /	4000 m
maximum 3000 m standards, spacifications, approvals certificate of suitability e RoHS conformity Yes reference code		500 m
standards, specifications, approvals certificate of suitability eRoHS conformity reference code according to IEC 81346-2 WH thes//support industry siemens.com/cs/ww/en/view/109766358 to website: Selection guide for cables and connectors to website: 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 of the support industry siemens.com/site of the sufficience of		1000 m
certificate of suitability Yes reference code WH • according to IEC 81346-2 WH • according to IEC 81346-2.2019 WHA further information / internet links Internet link • to website: Selection guide for cables and connectors https://support.industry.siemens.com/cs/ww/en/view/109766358 • to website: Industrial communication https://support.industry.siemens.com//simtlc.net • to website: Industrial communication https://support.industry.siemens.com/ • to website: Industry Online Support https://support.industry.siemens.com/ • to website: Industry Online Support https://support.industry.siemens.com security information security information https://support.industry.siemens.com security information 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 and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and an elevoriks. In order to protect plants, systems, machines and a nonecuton in necessary and only when appropriate security measures (e.g., firewalls and/or networks segmentation) are inplante. The adjust and solutions with industrial cybersens are used. Use of product versions that are no nontinuoustrial cybersecurity measures (e.g., firewalls and/or networks segmentation)		3000 m
• RoHS contomity Yes reference code - • according to IEC 81346-2. WH • according to IEC 81346-2.2019 WHA further information / internet link - • to website: Selection guide for cables and connectors https://support.industry.siemens.com/skiw/ien/view/109766358 • to website: Industrial communication https://www.siemens.com/skimalic.net • to website: Industrial communication https://www.siemens.com/skimalic.net • to website: Industrial communication https://www.siemens.com/csimalic.net • to website: Industrial communication https://www.siemens.com/csax • to website: CAx-Download-Manager https://www.siemens.com/csax • to website: Industry Online Support bites://systems.com/csax • to website: Industry Online Support Siemens provides products and solutions with industrial cybersecurity function security information / header security information Siemens provides products and solutions with industrial cybersecurity concept. Siemens provides and networks. Such systems, machines and networks against cyber theras, it is necessary to implement - an continuously maintain - a holisite, state-of-the-art industrial cybersecurity concept. Siemens provides and solutions with industrial cybersecurity concept. Siemens providus and networks segments in ordivers agremens industrial	standards, specifications, approvals	
reference code	certificate of suitability	
eacording to IEC 81346-2 WH eacording to IEC 81346-2:2019 WHA further information / internet links internet link o website: Selection guide for cables and connectors o web page: selection aid TIA Selection Tool bttps://www.siemens.com/istacloud io website: Industrial communication io website: Image database io website: Industry online Support intos://www.siemens.com/simatic.net io website: Image database io website: Industry online Support io cost Support io website: Industry online Support io cost Support io website: Industry online Support io cost Support io cost Support io cost Support io cost Support industry signenge.Com/Support industry signenge io website: Support Industry Siemenge industrial cybersecurity function that Support Industry on implement - and continuously maintain - a holistic, ior cost Support in systems, machines and networks such systems, machines and networks is cost systems, machines and networks in order to propriate security imeasures (c.g., firewalls and/or network segmentation are in place. For additional infor	RoHS conformity	Yes
eaccording to IEC 81346-2:2019 WHA further information / internet link internet link io website: Selection guide for cables and connectors https://www.siemens.com/cs/ww/en/view/109766358 io web page: selection aid TIA Selection Tool https://www.siemens.com/stacloud to website: Industrial communication io website: Industrial communication io website: Industrial communication io website: Industrial communication io website: Industrial communication to website: Industrial communication io website: Industrial communication io website: Industrial communication io website: Industry Online Support 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. Siemers' products and solutions constitute one element of such a concept. Clustomers are responsibil for preventing unautionized access to their plants, systems, machines and connection in ecossary and only when appropriate security measures that any be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens iproducts and solutions undergo continuous development to make them more secure. Siemens strong in ecossary and only when approdice security measures that any be inplemented, please visit www.siemens.com/cybersecurity	reference code	
further information / internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industrial communication • to website: Image database • to website: Industrial communication • to website: Industrial communication • to website: Industrial communication • to website: Industry Online Support • to website: Industry Online Support • to website: Industry Online Support security information Security information Security information Security information Security information Security information Inters://www.siemens.com/cax Number Support Security information Security information <td>-</td> <td>WH</td>	-	WH
Internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool https://www.siemens.com/tsticloud • to website: Industrial communication https://www.siemens.com/simatic.net • to website: Industry Online Support https://www.siemens.com/cax • to website: Industry Online Support https://www.siemens.com/cax • to website: Industry Online Support https://support.industry.siemens.com security information / header siemens provides products and solutions with industrial cybersecurity function security information 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 solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and onetworks. Such systems, machines and onetworks segmentation are in place. For additional information on industrial cybersecurity-industry. Siemens' products and solutions enterprise network ore their plants, systems, inconnees (e.g. f		WHA
 b website: Selection guide for cables and connectors https://support.industry.siemens.com/cs/ww/en/view/109766358 b web page: selection aid TIA Selection Tool https://support.industry.siemens.com/istacloud b website: Industrial communication https://sieportal.siemens.com/ b website: Image database b website: CAx-Download-Manager https://www.automation.siemens.com/cax b website: Industry Online Support https://support.industry.siemens.com/cax security information / header security information security information 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 and solutions constitute one element of such a concent. 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 entreprise network or the internet if and to the extent such a connection in network segmentation) are in place. For additional information on industrial cybersecurity reasures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity reasures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity reasures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity Resports that are no longer supported, and failure to apply the latest updates may increase subscribe to the Siemens industrial Cybersecurity RSS Feed under https://www.siemens.com/cett. (V4.7) 		
 to web page: selection aid TIA Selection Tool https://www.siemens.com/tstcloud to website: Industrial communication https://www.siemens.com/simatic-net to web page: SiePortal https://sieportal.siemens.com/ to website: Image database https://www.automation.siemens.com/bilddb to website: Industry Online Support https://www.siemens.com/cax to website: Industry Online Support https://www.siemens.com/cax to website: Industry Online Support security information / header security information to a rote to protect plants, systems, machines and networks and solutions with industrial cybersecurity function security information the easary 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 conponents should only be connected to an enterprise network or the internet if and to the extent such a connection in necessary and only when appropriate security. 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 are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. Costar informed about product updates subscribe to the Siemens industrial Cybersecurity RSS Feed under https://www.siemen		
• to website: Industrial communicationhttps://www.siemens.com/simatic-net• to web page: SiePortalhttps://sieportal.siemens.com/• to website: Image databasehttps://www.automation.siemens.com/bilddb• to website: CAx-Download-Managerhttps://www.siemens.com/cax• to website: Industry Online Supporthttps://www.siemens.com/cax• to website: Industry Online Supporthttps://support.industry.siemens.comsecurity information / headersecurity information 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 holisite, 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 solutions undergo continuously when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity consist and a solutions with segure security measures that may be implemented, please visit www.siemens.com/cybersecurity.exisons are used. Use of product versions are used. Use of 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)	-	
 to web page: SiePortal https://sieportal.siemens.com/ to website: Image database to website: CAx-Download-Manager https://www.automation.siemens.com/cax to website: Industry Online Support 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. 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 connection in necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity resists 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 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 Cyber		
• to website: Image database https://www.automation.siemens.com/bilddb • to website: CAx-Download-Manager https://www.siemens.com/cax • to website: Industry Online Support https://www.siemens.com/cax security information / header 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. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. Such 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 in networks segmentation) are in place. For additional information on industrial cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strong undergo continuous development to make them more secure. Siemens strong undergo continuous development to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates are no longer supported, and failure to apply the latest updates may increase customer's exposure to tyber threats. To stay informed about product updates 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 acustoribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)		
 to website: CAx-Download-Manager https://www.siemens.com/cax to website: Industry Online Support 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. In order to protect plants, systems, machines and networks. Su 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 in 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 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 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 Cybersecurit RSS Feed under https://www.siemens.com/cyter.(V4.7) 		
• to website: Industry Online Support https://support.industry.siemens.com security information / header 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 and solutions constitute one element – 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 onponents should only be connected to an enterprise network or the internet if and to the extent such a concept to an enterprise network or the internet if and to the extent such a connection in 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 that may be implemented, please visit www.siemens.com/cybersecurity are subject 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 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. 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 in 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 strong recommends that 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)	C C	
Security information Security information 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 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 in 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' product sand 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 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)	· · ·	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 i 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 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 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/cvert. (V4.7)	security information / header	
A margarele / Constitionation	security mormation	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	

CE EG-Konf.	Declaration of Con- formity	UK CA	() CCC	<u>Manufacturer Declara-</u> tion	
General Product Ap- proval	Marine / Shipping	other	Environment		
RCM	BUREAU VERITAS	Confirmation	<u>Confirmation</u>		

last modified:

8/9/2024 🖸