SIEMENS

Data sheet 6XV1822-5BH30

product type designation

product description

7/8 inch connecting cable

Plug-in cable (5-core), preferred length, preassembled with two 5-pole 7/8 inch male/female-contact connectors

7/8" plug-in cable for Power supply of the ET 200, pre-assembled cable with 2 7/8" connectors, 5-pole, 3 m.



suitability for use	Power supply of ET 200 modules with 7/8 inch power port to IP 65 degree of protection
cable designation	L-Y11Y-Z 5x1x1.5 GR
wire length	3 m
electrical data	
insulation resistance coefficient	1 GΩ·m
operating voltage / RMS value	600 V
conductor cross section / of the power line	1.5 mm²
continuous current / of the power lines	16 A
mechanical data	
number of electrical cores	5
type of electrical connection	7/8 inch - 180
outer diameter	
• of inner conductor	1.55 mm
 of the wire insulation 	2.73 mm
of cable sheath	10.5 mm
symmetrical tolerance of the outer diameter / of cable sheath	0.3 mm
design of stranding element	Pairs
conductor class	5
material	
 of the conductor 	CU, blank
 of the wire insulation 	PVC
of cable sheath	PUR
product component / PE connection	Yes
marking / of cores	Color, digits
color	
 of the power line insulation 	black
of cable sheath	gray
bending radius	
 with single bend / minimum permissible 	27 mm
 with multiple bends / minimum permissible 	63 mm
with continuous bending	75 mm
number of bending cycles	5000000; For use in cable carriers, for 5 million bending cycles with a bending radius of 75 mm, an acceleration of 4 m/s 2 and a speed of 180 m/min
tensile load / maximum	500 N
weight per length	149 kg/km
plug	
type of plug interlock	screwed

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 responsib 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 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 update subscribe to the Siemens Industrial Cybersecurity RSS Feed under	decise of alice in connection	7/0 inch 400	
ambient temperature - during poration - during storage - during installation - to minorat oil - to gresse radiological resistance / to UV radiation resistant product features, product functions, product components / general product feature, - halogen-free - halogen-free - halogen-free - sistion-free - No - sisting-free			
ambient temperature • during perature • during storage • during instalation fire behavior Flame-resistant acc. to IEC 60332-1 fere behavior Flame-resistant acc. to IEC 60332-1 resistant res		7/8 ITICTI	
during portation during storage during insport during installation during install			
during storage during transport during installation 40 480 °C during transport during installation 40 480 °C during transport during installation 40 480 °C during transport during installation fire behavior chemical resistance is to grease inclinated oil resistant resistant resistant resistant product floatures, product functions, product components / general product floatures, product functions, product components / general product floatures, product functions, product components / general product floature shadgen-free No silicon-free Standards, specifications, approvals ULETEL Isting / 300 V Rating Ves standards, specifications, approvals ULETEL Isting / 600 V Rating Ves certificate of suitability VEAC approval *Acid Sconformity *EAC approval *Acid Sconformity *Acid Sconform	·	40 0000	
during transport during installation during installation Free behavior Flame-resistant acc. to IEC 60332-1 chemical resistance in mineral oil it or grease resistant			
during installation fire behavior fire behavior in ordinary			
fire behavior Chemical resistance • to mineral oil • to grease radiological resistance / to UV radiation protection class IP product features, product functions, product components / general product feature • halogen-free • silicon-free • silicon-free • silicon-free • silicon-free • No ves • sundards, specifications, approvals ULJETIL isting / 300 V Rating ULJETIL style / 600 V Rating Ves • RoHS conformity • EAC approval • ROHS conformity Yes • certificate of suitability • LEAC approval • ROHS conformity Yes • certificate of suitability • LEAC approval • ROHS conformity Yes • according to IEC 81346-2-2019 • WDB further information / internet links • to website: Selection guide for cables and connectors • to web page: SiePortal • to website: Industrate communication • to website: Industrate or expension of plants, systems, machines and networks against cyber threats, it is necessary to implement — and continuously marian — a hoister, or and the province of plants, systems, machines and networks against cyber threats, it is necessary to implement — and continuously marian — a hoister, or and the properties of the properties and threating and threating and threating and threating and threati			
chemical resistance • to mineral oil • to grease radiological resistance / to UV radiation protection class IP product feature • halogen-free • halogen-f			
• to mineral oil • to grease radiological resistance / to UV radiation protection class IP product features, product functions, product components / general product feature • halogen-free • halogen-free • halogen-free • halogen-free • No • silicon-free Standards, specifications, approvals UL/ETL listing / 300 V Rating UL/ETL style / 800 V Rating Ves certificate of suitability • L2238 E300110 • Yes ROHS conformity • reference code • according to IEC 81346-2-2019 WDB Turther information / internet links • to web page: selection aguide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industry of support • to website: Industr		Flame-resistant acc. to IEC 60332-1	
resistant radiological resistance / to UV radiation resistant product features halogen-free halo			
radiological resistance / to UV radiation protection class IP product feature P65 / 67 product feature halogen-free No silicon-free No silicon-free No Standards, specifications, approvals UU-ETL listing / 300 V Rating No UU-ETL style / 600 V Rating Ves UU-ETL style / 600 V Rating Ves Cut-ETL style / 600 V Rati			
product feature, product feature halogen-free slicon-free slicon-free slicon-free slicon-free slicon-free halogen-free halogen-free slicon-free slicon-free slicon-free slicon-free slicon-free slicon-free halogen-free No Yes standards, specifications, approvals ULETL listing / 300 V Rating No ULETL style / 600 V Rating Ves certificate of suitability LU2238 E300110 Fer Agnetic of Suitability LU2238 E300110 Fer Agnetic of Suitability Fer Agnetic of Su			
product features, product functions, product components / general product feature			
product feature • halogen-free • silicon-free standards, specifications, approvals UL/ETL listing / 300 V Rating UL/ETL style / 600 V Rating Ves certificate of suitability • EAC approval • RoHS conformity reference code • according to IEC 81346-2:2019 WDB further information / internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: selection side at the selection standard to website: Image database • to website: Image starbase • to website: Image starbases • to website: Image sta	·		
* halogen-free	product features, product functions, product components / gen	neral	
Silicon-free Yes UL/ETL listing / 300 V Rating No UL/ETL syle / 600 V Rating Yes certificate of suitability EAC approval Yes RoHS conformity reference code according to IEC 81346-2:2019 WDB 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: Image database to website: CAx-Download-Manager to website: Industry Online Support thitps://www.siemens.com/simens.com/ security information Security information Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistry, state-of-the-art industrial cybersecurity function recessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on coessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on undergo continuous development to make them more secure. Siemens strond undergo continuous development to make them more secure. Siemens strond undergo continuous development on base them more secure. Siemens strond undergo continuous development to make them more secure. Siemens strond undergo continuous development to make them more secure. Siemens strond 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 the extent such a connection necessary and only when appropriate security measures de and them one secure. Siemens strond undergo continuous development to make them more secure. Siemens strond undergo continuous development to make th	product feature		
Standards, specifications, approvals ULETL listing / 300 V Rating Ves certificate of suitability EAC approval RoHS conformity reference code according to IEC 81346-2.2019 WDB 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: Industrial communication to website: Industry Online Support thttps://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/simatic-net https://www.siemens.com/cs/wwienens.com/biddb https://www.siemens.com/cs/wwienens.com/biddb https://www.siemens.com/cs/wwienens.com/cs/ww	-		
ULETL isleting / 300 V Rating ULETL style / 600 V Rating Yes erificate of suitability EAC approval RoHS conformity Yes RoHS conformity Yes reference code • according to IEC 81346-2:2019 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: Industrial communication • to website: CAx-Download-Manager • to website: Industry Online Support security information Security information Security information Security information Security information Security information Siemens provides products and solutions with industrial cybersecurity 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 and networks. Such systems, machines and networks. Such systems, such and networks. Such systems, machines and networks and networks. Such systems, machines and networks. Such systems,	• silicon-free	Yes	
UL/ETL style / 600 V Rating Certificate of suitability EAC approval RoHS conformity reference code according to IEC 81346-2:2019 WDB further information / internet links internet link to website: Selection guide for cables and connectors to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: Image database to website: Industry Online Support to website: Industry Online Support Security information security information 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 networks. Such systems, and connection necessary to implement—and continuously maintain—a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions ountifute one element of such a concept. Customers are responsib for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks such a concept. Customers are responsib for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks such acconnection necessary and only when appropriate security measures (e.g. firewalls and/on networks. Such systems, machines and networks such as concept. Customers are responsib for preventing unauthorized access to their plants, systems and components should only be connected to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/on 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 should only be a necessary and only when appropriate security measures (e	standards, specifications, approvals		
certificate of suitability EAC approval RoHS conformity reference code according to IEC 81346-2:2019 WDB further information / internet links internet link to website: Selection guide for cables and connectors to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: Industrial communication to website: Image database to website: Industry Online Support thtps://www.siemens.com/simatic-net https://www.automation.siemens.com/bilddb https://www.automation.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://www.automation.siemens.com/simatic-net https://www.automation.siemens.com/simatic-net https://www.automation.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://www.automation.siemens.com/simatic-net https://www.automation.siemens.com/cax https://www.automation.siemens.com/simatic-net https://www.automation.siemens.com/cax https://www.automation.com/cax https://www.automation.siemens.com/cax https://www.au	UL/ETL listing / 300 V Rating	No	
EAC approval	UL/ETL style / 600 V Rating	Yes	
reference code	certificate of suitability	UL2238 E300110	
reference code according to IEC 81346-2:2019 further information / internet links internet link to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: SiePortal to web page: SiePortal to website: Industrial communication to website: Image database to website: Image database to website: Image database to website: Industry Online Support https://swww.siemens.com/simatic-net https://swww.siemens.com/bilddb https://swww.siemens.com/cax https://swport.industry.siemens.com/bilddb https://swport.industry.siemens.com/simatic-net https://swport.industry.siemens.com/cax https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/cax https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/cax https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/simatic-net https://support.industry.siemens.com/bilddb htt	 EAC approval 	Yes	
ording to IEC 81346-2:2019 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: Image database to website: CAx-Download-Manager to website: Industry Online Support 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 responsib for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and onetworks. Such systems, machines and onetworks. Such systems, machines and networks. Such systems, machines and onetworks or the internet if and to the extent such a connection 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 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 update subscribe to the Siemens industrial cybersecurity informed about product update subscribe to the Siemens industrial cybersecurity informed about product update subscribe to the Siemens industrial cybersecurity RSS SF eed under	RoHS conformity	Yes	
internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: SelePortal • to web page: SelePortal • to website: Image database • to website: Image database • to website: Industry Online Support Security information security information Siemens provides products and solutions with industrial cybersecurity function that support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary in 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 responsib for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connecte to an enterprise networ the internet if and to the extent such a connection 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 update subscribe to the Siemens Industrial Cybersecurity RSS Feed under	reference code		
intermet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web page: SiePortal • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industrial 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 and solutions constitute one element of such a concept. Customers are responsib 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 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 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	• according to IEC 81346-2:2019	WDB	
to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Industrial communication to website: Image database to website: Image database to website: CAx-Download-Manager to website: Industry Online Support security information 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 concept. Customers are responsib 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 necessary and only when appropriate security measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/on network segmentation) are used. Use of product versions that are no longer su	further information / internet links		
to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal to website: Image database to website: Image database intps://www.automation.siemens.com/ to website: Image database intps://www.automation.siemens.com/bilddb https://www.siemens.com/cax https://www.siemens.com/cax https://www.siemens.com/cax https://www.siemens.com/cax https://www.siemens.com 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 necessary and only 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 strong recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of products are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product update subscribe to the Siemens Industrial Cybersecurity RSS Feed under	internet link		
to website: Industrial communication to web page: SiePortal to website: Image database https://www.automation.siemens.com/bilddb to website: CAx-Download-Manager to website: Industry Online Support security information Security information 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 responsib for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connecte to an enterprise network or the internet if and to the extent such a connection necessary and only when appropriate security measures (e.g. firewalls and/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 update subscribe to the Siemens Industrial Cybersecurity formed about product update subscribe to the Siemens Industrial Cybersecurity formed about product update subscribe to the Siemens Industrial Cybersecurity formed about product update subscribe to the Siemens industrial Cybersecurity formed about product update subscribe to the Siemens Industrial Cybersecurity formed about product	 to website: Selection guide for cables and connectors 	https://support.industry.siemens.com/cs/ww/en/view/109766358	
to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support 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 responsib for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one 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	 to web page: selection aid TIA Selection Tool 	https://www.siemens.com/tstcloud	
• to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • to website: Industry Siemens.com • to website: Industry Siemens.com/ • to website: Industry Siemens industrial 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 update subscribe to the Siemens Industrial Cybersecurity RSS Feed under	 to website: Industrial communication 	https://www.siemens.com/simatic-net	
• to website: CAx-Download-Manager • to website: Industry Online Support **security information** 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 responsib 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 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	to web page: SiePortal	https://sieportal.siemens.com/	
• to website: Industry Online Support Security information	to website: Image database	https://www.automation.siemens.com/bilddb	
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 responsib 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 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	• to website: CAx-Download-Manager	https://www.siemens.com/cax	
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 responsib 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 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	• 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 responsib 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 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 update subscribe to the Siemens Industrial Cybersecurity RSS Feed under	security information		
nups.//www.siemens.com/cert. (v4.7)	security information	threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates,	

Approvals / Certificates

General Product Approval

Environment





Declaration of Conformity



Manufacturer Declaration Confirmation

Industrial Communication

PROFINET

last modified:

8/18/2024