SIEMENS

Data sheet 6XV1875-5AH50

product type designation

product description

antenna connection cable N-Connect plug/plug

Connecting cable for SIMATIC NET antennas, preassembled

N-Connect male/male flexible connection cable pre-assembled; length 5 m flexible cable, for example, for the connection to antennas, suitable for IWLAN and mobile radio.



| suitability for use | Flexible connecting cable for connecting an antenna or RCoax cable to a SCALANCE M/W |
|---|--|
| wire length | 5 m |
| electrical data | |
| number of electrical connections | 2 |
| type of electrical connection | N-Connect/N-Connect male/male |
| transmission frequency | 0 6000 MHz |
| attenuation factor per length | |
| • at 2.4 GHz / typical | 0.53 dB/m |
| at 5.2 GHz / typical | 0.83 dB/m |
| • at 5.85 GHz / typical | 0.89 dB/m |
| return loss | |
| • minimum | 23 dB |
| impedance | |
| • rated value | 50 Ω |
| capacity per length / at 1 kHz | 82 pF/m |
| relative speed | 82 % |
| mechanical data | |
| design of the shield | Braided shield made of tin-plated copper wires |
| outer diameter | |
| of inner conductor | 1.4 mm |
| • of dielectric | 3.8 mm |
| of cable sheath | 6.3 mm |
| symmetrical tolerance of the outer diameter / of cable sheath | 0.2 mm |
| thickness / of cable sheath | 0.76 mm |
| material | |
| of inner conductor | Cu |
| • of dielectric | polyethylene foam |
| of cable sheath | FRNC |
| color | |
| of cable sheath | pastel turquoise |
| bending radius | |
| with single bend / minimum permissible | 32 mm |
| with multiple bends / minimum permissible | 45 mm |
| tensile load / maximum | 80 N |
| weight per length | 75 kg/km |
| ambient conditions | |
| ambient temperature | |

| during stratage during transport during installation during stratage during transport during installation during statlation during statlation s | | |
|--|---|--|
| during transport during installation chemical resistance vio mineral oil conditional resistance vio mineral oil resistant product features, product functions, product components / general product features, product functions, product components / general product features via piscon-free vision-free | during operation | -40 +80 °C |
| during installation | during storage | -40 +80 °C |
| chemical resistance • to mineral oil conditional resistance • to mineral oil resistant protection class IP product features • halogen-free • halogen-free • halogen-free • halogen-free • halogen-free • salicon-free Standards, spocifications, approvals certificate of suitability • EAC approval • ROHS conformity • EAC approval • for protection in accordance with EN 45545-2 No standard • for fire behavior / flame resistance UL 1685 (Vertical tray), UL 1581 Sec. 1080 (H) reference code • according to IEC 81346-2 • according to IEC 81346-2 • WG • according to IEC 81346-2 • 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 website: Industrial points of the selection Tool • to website: Industry Online Support security information Approvals / Certificates | during transport | -40 +80 °C |
| e to mineral oil product features, product functions, product components / general product features, product functions, prod | during installation | -25 +80 °C |
| radiological resistance / to UV radiation protection class IP product features, product functions, product components / general product feature | chemical resistance | |
| protection class IP product features, product functions, product components / general product feature | to mineral oil | conditional resistance |
| product features, product functions, product components / general product feature | radiological resistance / to UV radiation | resistant |
| product feature | protection class IP | IP68; when plugged in |
| * halogen-free * Yes * silicon-free Yes * yes * silicon-free * Yes * y | product features, product functions, product components / gen | neral |
| e silicon-free standards, specifications, approvals certificate of suitability EAC approval RoHS conformity for grotection in accordance with EN 45545-2 No standard for fire behavior / flame resistance freference code according to IEC 81346-2 according to IEC 81346-2:2019 WGB 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 website: Image database Security information Approvals / Certificates Approvals / Certificates Yes Yes Yes No Yes Yes Ves UL 1685 (Vertical tray), UL 1581 Sec. 1090 (H) WGB WGB WGB HUBS://support.industry, siemens.com/cs/ww/en/view/109766358 https://support.industry.siemens.com/cs/ww/en/view/109766358 https://support.industry.siemens.com/sicloud https://sww.automation.siemens.com/bilddb https://sww.automation.siemens.com/bilddb https://sww.automation.siemens.com/bilddb https://www.siemens.com/cax to web site: chart industry opines support industry siemens.com Security information Security information Security information Security information Approvals / Certificates Approvals / Certificates | product feature | |
| standards, specifications, approvals certificate of suitability • EAC approval • RoHS conformity • fire protection in accordance with EN 45545-2 No standard • for fire behavior / flame resistance • according to IEC 81346-2 • 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 website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support Security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, in order to protect plants, systems, machines and networks and networks. In order to protect plants, systems, machines and networks and networks. Such systems, scompt. Systems, provides access to the inject secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a hoistic, state-of-the-air industrial cybersecurity concept. Siemens provides and solutions constitute one element of such a concept. Customers are responsible for preventing unauthroized access to the protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a hoistic, state-of-the-air industrial cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthroized access to the products and solutions or industrial cybersecurity concept. Siemens products and networks against cyber threats, it is necessary to implement – and continuously maintain – a hoistic, state-of-the-air dustrial cybersecurity concept. Siemens products and networks against cyber threats. To seven the mana | halogen-free | Yes |
| certificate of suitability • EAC approval • RoHS conformity • fire protection in accordance with EN 45545-2 standard • for fire behavior / flame resistance • for fire behavior / flame resistance • according to IEC 81346-2 • according to IEC 81346-2-2019 **WGB **UL 1685 (Vertical tray), UL 1581 Sec. 1090 (H) **Teference code • according to IEC 81346-2-2019 **WGB **Internet link • to website: Selection guide for cables and connectors • to web page: Selection guide for cables and connectors • to web page: Selection aid TIA Selection Tool • to web page: Selection aid TIA Selection Tool • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support **Intos://www.siemens.com/cs/ww/en/view/109766358 **Intos://www.siemens.com/cs/ww/en | • silicon-free | Yes |
| ROHS conformity Fire protection in accordance with EN 45545-2 No standard • for fire behavior / flame resistance UL 1685 (Vertical tray), UL 1581 Sec. 1090 (H) reference code • according to IEC 81346-2 • according to IEC 81346-2 • according to IEC 81346-2:2019 WGB 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 website: Image database • to website: Industry Opinine Support • to website: Industry Opinine Support bittps://www.siemens.com/sticloud https://www.siemens.com/siemens.com/bilddb https://www.siemens.com/cax bittps://www.siemens.com/cax https://www.siemens.com/siemen | standards, specifications, approvals | |
| RoHS conformity Internation Roman Script Standard For fire behavior / flame resistance Freference code According to IEC 81346-2 According to IEC 81346-2 Book WGB Further information / internet links Internet link Interne | certificate of suitability | |
| standard • for fire behavior / flame resistance • for fire behavior / flame resistance • according to IEC 81346-2 • to web stee: 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 website: Image database • to website: Image database • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support bittps://www.siemens.com/cax • 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 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. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks against cyber threats, it is necessary and only when appropriate security measures (e.g. frewalls and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens broud 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) | EAC approval | Yes |
| e for fire behavior / flame resistance • according to IEC 81346-2 • according to IEC 81346-2 • according to IEC 81346-2.2019 **WGB **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 website: Image database • to website: CAx-Download-Manager • to website: Image database • 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 functions that support the secure operation of plants, systems, machines and networks in order to protect plants, systems, machines and networks attace-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 networks segmentation) are in place. For additional information on industrial cybersecurity measures what 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 RBS Feed under | RoHS conformity | Yes |
| • for fire behavior / fiame resistance reference code | • fire protection in accordance with EN 45545-2 | No |
| reference code according to IEC 81346-2 according to IEC 81346-2:2019 WGB 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 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 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 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 is necessary and only when appropriate security measures (e.g. firewalls and/or networks seguration) are place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/corporates 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 com/cert. (V4.7) | standard | |
| according to IEC 81346-2: WG according to IEC 81346-2: 2019 WGB 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 website: Image database • to website: Image database • to website: Industry Online Support Security information 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 under 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.slemens.com/cybersecurity-industry. Slemens' 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 Slemens industrial Cybersecurity RSS Feed under https://www.slemens.com/cert. (V4.7) | • for fire behavior / flame resistance | UL 1685 (Vertical tray), UL 1581 Sec. 1090 (H) |
| **according to IEC 81346-2:2019 **further Information / Internet links** internet link **to 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: SiePortal **to website: Image database **to website: Image database **to website: Industry Online Support **to website: Industry Online Support **security information** **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, and incess and networks, and solutions constitute one element of such a concept. Usemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks 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 that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that please so the please story 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/cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Fee | 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 web page: SiePortal • to website: Image database • to website: Industry Online Support • to website: Industry Online Support | according to IEC 81346-2 | WG |
| internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: SiePortal • 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 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. Clustomers 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 (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 (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 product versions are applied as soon as they ar | according to IEC 81346-2:2019 | WGB |
| to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Image database to website: Image database to website: Industry Online Support to website: Industry Online Support security information Security information 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 the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product updates are applied as soon as they are available and that the latest product updates are subscribed to a ply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates | further information / internet links | |
| to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Image database to website: Image database to website: CAx-Download-Manager to website: CAx-Download-Manager to website: Industry Online Support thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://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, nechtors of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, nechtors of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, nechtors of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, nechtors 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 cu | internet link | |
| to web page: SiePortal 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 functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement — and continuously maintain — a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens. com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates | • to website: Selection guide for cables and connectors | https://support.industry.siemens.com/cs/ww/en/view/109766358 |
| 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 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 onetworks. Such systems, machines and onetworks 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 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: selection aid TIA Selection Tool | https://www.siemens.com/tstcloud |
| to website: CAx-Download-Manager to website: Industry Online Support security information Security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates | • to web page: SiePortal | https://sieportal.siemens.com/ |
| • 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. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates | to website: Image database | https://www.automation.siemens.com/bilddb |
| security information Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates | • to website: CAx-Download-Manager | https://www.siemens.com/cax |
| 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 | |
| | security information | that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under |
| General Product Approval Environment | ·· | |
| | General Product Approval | Environment |







Confirmation

last modified:

8/8/2024