## **SIEMENS**

## **Data sheet**

## 6AG1961-3BA01-7AA0



## SIPLUS SITOP PS MODULAR Puffermodul

SIPLUS PS modular buffer module based on 6EP1961-3BA01 with conformal coating, -25...+70 °C, for 6EP1x3x-3BAx0 buffer time 100 ms to 10 s depending on load current

Figure similar

supply voltage at DC rated value	24 V	
input voltage at DC	24 28.8 V	
nemory		
design of the mains power cut bridging-connection	Backup time: with 40 A load current: 200 ms; with 20 A load current: 400 ms; with 10 A load current: 800 ms; with 5 A load current: 1.6 s. Reduces the backup time by 100 ms in combination with 6EP1 437-3BA10. Maximum backup time 100 ms in combination with 6EP1 336-2BA10 (load current 20 A	
buffering time in the event of power failure	0.16 min	
utput		
formula for output voltage	Vin - approx. 1 V	
output current		
rated value	40 A	
rotection and monitoring		
display version		
• for normal operation	Green LED for "supply voltage > 20.5 V"	
nterfaces		
product component PC interface	No	
product function communication function	No	
design of the interface	without	
afety		
galvanic isolation between input and output	Yes	
operating resource protection class	Class III	
protection class IP	IP20	
standard		
<ul> <li>for emitted interference</li> </ul>	EN 55022 Class B	
• for interference immunity	EN 61000-6-2	
tandards, specifications, approvals		
certificate of suitability		
CE marking	Yes	
MTBF at 40 °C	2 538 071 h	
mbient conditions		
ambient temperature		
<ul> <li>in horizontal mounting position during operation</li> </ul>	-25 +70 °C; with natural convection	
- during transport	-40 +85 °C	
during transport	-40 +85 °C	
during transport     during storage	-40 +85 °C	
	-40 +85 °C 6 000 m	

type of electrical connection	relative humidity with condensation according to IEC 60068-2-	100 %; RH incl. condensation/frost (no commissioning if condensation is	
resistance to biologically active substances conformity according to Rn O272-3-3 resistance to chemically serve substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to biologically active substances conformity according to Rn O272-3-3 resistance to biologically active substances conformity according to Rn O272-3-3 resistance to biologically active substances conformity according to Rn O272-3-3 resistance to rechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically active substances conformity according to Rn O272-3-3 resistance to mechanically according to Rn O272-3 resistance to mechanically according t			
resistance to chemically active substances conformity according to 10 to	·		
resistance to mechanically active substances conformity according to EN 60713-3.  Yes, Class 384 ind. sand, dust according to EN 60713-3.  Yes, Class 68.2 mold, fungal, sponge spores (except fauna) according to EN 60713-3.  Yes, Class 68.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels of the continually active substances conformity according to EN 67071-3.6  Yes, Class 68.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 (RH < 75%) incl. salt spray acc. to EN 6068-2-52 (severity levels) according to EN 67071-3.6  Yes, Class 65.3 incl. salt dust  Yes, Class 65.3	<u> </u>	·	
according to EN 60721-3-3 resistance to bilogically adve substances conformity according to EN 60721-3-6 resistance to bridge printed circuit board according to EN 60721-3-6 resistance to chamically active substances conformity according to EN 60721-3-6 resistance to chamically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity according to EN 60721-3-6 resistance to chamically active substances conformity according to EN 60721-3-6 resistance to chamically active substances conformity according to EN 60721-3-6 resistance to chamically active substances conformity according to EN 60721-3-6 resistance and according to EN 60721-		level 3)	
recisione to themically active substances conformity according to EN 60721-3-6 resistance to themically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity according to EN 60721-3-6 resistance to mechanically active substances conformity by end coating of equipped printed circuit board according to EN 60721-3-6 resistance to EN 60721-3-6 resistance to according to EN 60721-3-6 resistance to according to EN 60721-3-6 resistance to EN 607	according to EN 60721-3-3	Yes; Class 354 Incl. sand, dust	
to EN 60721-3-6 level 3) level 3) resistance to mechanically active substances conformity according to EN 60721-3-6 screening for equipped printed circuit board according to EN 60721-3-6 stock 51086 Yes; Class 6S3 incl. sand, dust according to EN 60721-3-6 stock 51086 Yes; Class 6S3 incl. sand, dust according to EN 60084-3 Yes; Class 2 for high availability yeo of coating protection against pollution according to EN 60084-3 Yes; Discoloration of the coating during service life possible product conformity of the coating Qualification and Performance of Electrical Insulating Compound for Printed Board Assemblies according to IPC-CC-300A acromection method type of electrical connection  • at input • at output • 1 screw terminal • 1 screw terminal • 1 screw terminal for 0.5 10 mm² • at output • 1 screw terminal for 0.5 10 mm² • at output • 1 screw terminal for 0.5 10 mm² • the control of the coating during service life possible  Provided spacing • top • 50 mm  • left • 0 mm • left • 0 mm • left • 0 mm • left • 1 mminimizer • 2 mminimizer • 3 mminimizer • 4 mminimizer • 1 to website: Industry Mall • 1 to website: Industry		Yes; Class 6B2 mold, fungal, sponge spores (except fauna)	
according to equipped printed circuit board according to EN 61086 Yes; Class 2 for high availability 61086 Yes; Type 1 protection guarant pollution according to EN 60864.3 Yes; Type 1 protection 9, 1994 Per 1 protection 1			
yes (Type 1) protection 60664-3 Yes; Type 1) protection 60664-3 Yes; Discolaration of the coating according to MIL-146058C Yes; Discolaration of the coating during service life possible product conformity of the coating Qualification and Performance of Electrical Insulating Compound for Printed Board Assemblies according to IPC-CC-330A onnection method ype of electrical connection • at input • at output • 1 screw terminal • at output • 1 screw terminal for 0.5 10 mm² • at output • 1 screw terminal for 0.5 10 mm² • at output • 10 x 125 x 121 mm insulatation width × mounting height required spacing • top • bottom • bottom • left • onm • right • onm • infall • standard rail mounting • x 37 x 125 x 121 mm insulatation width × mounting height required spacing • top • bottom • onm • left • onm • infall • standard rail mounting • x 37 rail mounting • x 48 yes • x 49 yes • x 57 rail mounting • x 49 yes • x 57 rail mounting • x 49 yes • x 57 rail mounting • x 49 yes • x 57 rail mounting • x 40 yes • x 57 rail mounting • x 40 yes • x 57 rail mounting • x 58 yes • x 59 yes • x 50		Yes; Class 6S3 incl. sand, dust	
yes, Discoloration of the coating during service life possible  yes, Discoloration of the coating during service life possible  yes, Conformal Coating, Class A  yes, Class A  yes, Conformal Coating,		Yes; Class 2 for high availability	
product conformity of the coating Qualification and Performance of Electrical Insulating Compound for Printed Board Assemblies according to IPC-CC-830A  pype of electrical connection		Yes; Type 1 protection	
of Electrical Insulating Compound for Printed Board Assemblies according to IP-CC-G-30A  onnection method  type of electrical connection	type of test of the coating according to MIL-I-46058C	Yes; Discoloration of the coating during service life possible	
type of electrical connection	product conformity of the coating Qualification and Performance of Electrical Insulating Compound for Printed Board Assemblies	· · · · · · · · · · · · · · · · · · ·	
at input at output behanical data width × height × depth of the enclosure installation width × mounting height at op at op at op at op bottom bottom bottom at one at op bottom at output at op bottom at output at out	connection method		
at input at output behanical data width × height × depth of the enclosure installation width × mounting height at op at op at op at op bottom bottom bottom at one at op bottom at output at op bottom at output at out	type of electrical connection	screw terminal	
width × height x depth of the enclosure 70 × 125 × 121 mm installation width × mounting height 70 × 225 mm 70 × 22			
width × height × depth of the enclosure installation width × mounting height 70 × 225 mm  70 × 2	mechanical data		
Installation width × mounting height  required spacing  • top  • bottom  • bottom  • left  • right  fastering method  • standard rail mounting  • S7 rail mounting  • val  • val mounting  • val  • val mounting  • val  • val mounting  • val  • to website: Industry Online Support  dollitonal Information  other information  other 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. Such systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, slate-of-the-art industrial cybersecurity mounts and networks eigenens continuous development on such security measures that as upport the secure operation of plants, systems, machines and networks. Such systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, slate-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a continuously maintain – a holistic, slate-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a perioducts and solutions on constitute one element of such a perioducts and solutions constitute one element of such a perioducts and solutions constitute one element of such a perioducts and solutions constitute one element of such a perioducts and solutions constitute one element of such a perioducts and solutions constitute one element of such a perioducts and solutions constitute one element of such a such season and networks. Such systems, machines and networks under such such season machines and element of such a such season and such season and such such season and season and such season and such season and season and season and		70 × 125 × 121 mm	
required spacing  • top • bottom • bett • right • or mm • left • or mm • right • or mm fastening method • standard rail mounting • S7 rail mounting • S7 rail mounting • No • wall mounting • No housing can be lined up net weight • 1.2 kg  **The information internet links **Internet link • to website: Industry Mall • to website: Industry Online Support  **The formation  **The formation  **The formation  **The formation  **Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  **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 entworks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. 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 or 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 that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber hreats. To Tosty informed about product updates, subscribe to the Siemens I		70 × 225 mm	
• top     • bottom     • bottom     • left     • right     • right     • onm  fastening method     • Sanps onto DIN rail EN 60715 35x7.5/15  • standard rail mounting     • S7 rail mounting     • No     • wall mounting     • No housing can be lined up     net weight     1.2 kg     ruther information internet links     • to website: Industry Mall     • to website: Industry Mall     • to website: Industry Online Support     ditional information  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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, sagainst cyber threats, it is necessary to implement – and continuously maintain – a holistic state-of-the-art industrial cybersecurity products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to longer. Siemens products and networks. Such systems, machines and networks, such as and networks. Such systems, machines and networks and networks. Such systems, machines and networks repending unauthorized access to report parts, systems, machines and networks repending unauthorized access to report singer products and solutions on sonstitute one element of such a concept. Customers are responsible for preventing unauthorized access to report singer such as connection is necessary and only when appropriate security measures (e.g., firewalls and/or networks segmentation) are in place. For singer products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates as may lorease customer's exposure to cyber fireats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/concert. (14.7.1).			
bottom     ielet		50 mm	
Interest of the security information  Information  Security information  Security information  Security information  Security information  Interest of the security states of the security oncept. Signers products and solutions with industrial cybersecurity measures for connection is necessary and only when appropriate security measures (e.g. firewalls and/or networks. Subners) are repose solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates, subscribe to the Siemens product and solutions are already recommends that pop product plants and one thought and one tworks against cybersecurity concept. Siemens products and solutions concept. Customers are responsible for preventing unabtriated peace with a subnormal prevention and networks. Such systems, machines and networks against cybersecurity concept. Siemens products and solutions constitute one element of such a concept. Customers are responsible for preventing unabtriated eyes and only when appropriate security measures (e.g. firewalls and/or networks. Segments products and solutions constitute one element of such a concept. Customers are responsible for preventing unabtriated eyes can be plants, systems, machines and networks. Such systems, machines and networks against cybersecurity measures to their plants, systems, such ness 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 or not prevent the secure operation of parts, 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 or notation or notation or notation or notation or notati	•		
in right			
fastening method  • standard rail mounting  • ST rail mounting  • wall mounting  • wall mounting  housing can be lined up  res  reformation internet links  internet link  • to website: Industry Mall  • to website: Industry Mall  • to website: Industry Online Support  thtps://support.industry.siemens.com  other information  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  ecurity information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, in order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Slemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Slemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/certs. To stay informed about product updates, subscribe to the Slemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (v4.7.7)			
standard rail mounting     S7 rail mounting     No     wall mounting     No     No     No     No     No     Nosing can be lined up     Yes     net weight     1.2 kg     urther Information internet links     internet link     • to website: Industry Mall     • to website: Industry Mall     • to website: Industry Online Support     dditional information      other information      Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)      ecurity 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 retworks 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 elemen's received threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one elemen's received to an enterprise network or their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or their 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 that are no longer supported, and failurated cybersecurity resources contributed 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			
Solutions and be lined up  wall mounting  No  housing can be lined up  Yes  net weight  1.2 kg  writher information internet links  internet link  to website: Industry Mall to website: Industry Online Support  https://mall.industry.siemens.com  https://support.industry.siemens.com  to website: Industry Online Support  https://support.industry.siemens.com  ddittional information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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 one proportion of plants in a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one proportion and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that product versions are used. Use of product sand solutions undergo continuous development to make them more secure. Siemens strongly recommends that product versions are used. Use of product versions that are no longer supported, and failutes to apply the latest updates way 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)	•		
• wall mounting housing can be lined up retweight 1.2 kg  Internet link  • to website: Industry Mall • to website: Industry Mall • to website: Industry Online Support  Internet link  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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 eyesecurity conept. 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 through one how it is necessary and only when appropriate security measures through one how it is necessary and only when appropriate security measures through one how it is necessary and only when appropriate security measures through one how it is necessary and only when appropriate security measures through one how it is necessary and only when appropriate security measures through one how it is necessary and only when appropriate security measures it house 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 threa	-		
housing can be lined up  Yes  net weight  1.2 kg  urther information internet links  internet link  • to website: Industry Mall • to website: Industry Online Support  https://mall.industry.siemens.com  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  security information  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 inplement – and continuously maintan – 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 concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and oncopenents should only be connected to an enterprise network on 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 develorment 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/cetr. (V4.7)	· ·		
net weight 1.2 kg  Internet link  In			
internet link  Internet lindustry Mall  Internet lindustry Online Support  Internet lindustry Online Support  Internet lindustry.siemens.com  Interne			
internet link  • to website: Industry Mall  • to website: Industry Online Support  https://support.industry.siemens.com  https://support.industry.siemens.com  dditional information  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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 rease 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)		1.2 kg	
• to website: Industry Mall • to website: Industry Online Support    https://support.industry.siemens.com	further information internet links		
• to website: Industry Online Support  dditional information  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  ecurity 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-fhe-art industrial cybersecurity concept. Siemens' products and solutions constitue one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	internet link		
other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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)	<ul><li>to website: Industry Mall</li></ul>	https://mall.industry.siemens.com	
other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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)	<ul> <li>to website: Industry Online Support</li> </ul>	https://support.industry.siemens.com	
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)	additional 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)	other 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)	security information		
• • • • • • • • • • • • • • • • • • • •	security information	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	
(assitications	Classifications	.,	

	Version	Classification
eClass	14	27-04-07-05
eClass	12	27-04-07-05
eClass	9.1	27-04-07-05
eClass	9	27-04-07-05
eClass	8	27-04-06-90
eClass	7.1	27-04-06-90
eClass	6	27-04-06-90
ETIM	9	EC000382
ETIM	8	EC000382
ETIM	7	EC000382
IDEA	4	4149
UNSPSC	15	39-12-10-11

Approvals Certificates

**General Product Approval** 

**EMV** 

Miscellaneous



Manufacturer Declara-tion





<u>KC</u>

EMV



last modified:

6/24/2024

