# **SIEMENS**

## **Data sheet**

6EP4295-8HB00-0XY0



#### SITOP BUF8600/10S/40A

SITOP BUF8600 10s buffer module for PSU8600 buffer capacity 10 s/40 A with dual-layer capacitators maintenance-free

memory		
type of energy storage	Double-layer capacitors	
design of the mains power cut bridging-connection	Backup time with 40 A load current: 10 s	
buffering time for rated value of the output current in the event of power failure	10 000 ms	
load time typical	10 min; at 400 V	
output		
output current		
• rated value	40 A	
protection and monitoring		
display version	3-color LED for operating state module	
<ul> <li>for normal operation</li> </ul>	LED green for "buffer standby exist"	
• in buffering mode	LED yellow for "buffered mode"	
interfaces		
product function communication function	Yes	
design of the interface	Ethernet/PROFINET via power supply unit PSU8600	
safety		
operating resource protection class	Class III	
protection class IP	IP20	
standard		
• for emitted interference	EN 55022 Class B	
• for interference immunity	EN 61000-6-2	
standards, specifications, approvals		
certificate of suitability		
CE marking	Yes	
UL approval	Yes; cULus-Listed (UL 508, CSA C22.2 No. 107.1), File E197259	
CSA approval	Yes; cCSAus (CSA C22.2 No. 62368-1, UL 62368-1)	
<ul> <li>EAC approval</li> </ul>	Yes	
• SEMI F47	Yes	
type of certification CB-certificate	Yes	
MTBF at 40 °C	1 190 747 h	
standards, specifications, approvals hazardous environments		
certificate of suitability		
• ATEX	No	
• cCSAus, Class 1, Division 2	No	
standards, specifications, approvals marine classification		
shipbuilding approval	Yes	
Marine classification association		
<ul> <li>American Bureau of Shipping Europe Ltd. (ABS)</li> </ul>	Yes	
<ul> <li>Det Norske Veritas (DNV)</li> </ul>	Yes	

antherit interporture	ambient conditions					
- Authing seration     - Authing storage     - Authority of Control and Salaus message     - Authority of Control and Salaus an						
• during startage     environmental category according to IEC 60721     Commister dates 3K3, 5 95% no condensation     Commister dates 3K3, 5 95% no condensation     Pugain terminal with screw connectors           • K1, 22 (control contact) and 12,14, 22,24 (message signals): 1 screw terminal each for 20 2 1.5 mm²	·	-25 +60 °C: with natural conv	vection			
• Auring storage						
environmental category according to IEC 60721  Cinnate class 3K3, S 96% no condensation  The control cincuit and attack message act for 0.2 15 mm?  Flug-in terminal with screw connectors  X1, X2 (control contact) and 13, 14, 23, 24 (message signals): 1 screw terminal script for 0.2 15 mm?  Suitability for interaction modular system  Yes  Bype of comerction to system components  Will integrated connector  With x legit x depth of the enclosure  Installation with x mounting height  125 x 255 mm  required spaning  I op  So mm  I of m						
type of electrical connection  • for control circuit and status mossage suitability for interaction modular system type of connection to system components type of connection		Climate class 3K3, 5 95% no	condensation			
**In a control circuit and status message   X1, X2 (control contract) and 13,14, 23, 24 (message signals): 1 screw terminal each for 02,1,5 mm²	connection method					
sultability for interaction modular system Yes Sype of connection to system components With x height x depth of the endosure installation width x mounting height 125 x 225 mm required spacing • top • bottom • left • om • height O mm • standard rail mounting • register • Standard rail mounting • Yes • Standard rail mounting • Xes • Standard rail mounting • Yes • Standard rail mounting • No • wall mounting • No • wall mounting • No  note weight 1.95 kg • Security information • Internet links • to website: Industry Mall • to website: Industry Online Support • to website: Industry Chine Support • Security information • Security	type of electrical connection	Plug-in terminal with screw con	nectors			
Type of connection to system components  Wis integrated connector  mischanical data  width * height × depth of the enclosure installation width × mounting height  125 × 225 mm  required spacing  100  • bottom • left • 0 mm • left • 0 mm • signt  30 mm  50 mm  50 mm  6 standard rail mounting  • standard rail mounting  • standard rail mounting  • val mounting  No  • bottom • left • mounting  No  • wal mounting  No  housing can be lined up  Yes  mechanical accessories  mechanical acce	for control circuit and status message		X1, X2 (control contact) and 13,14, 23, 24 (message signals): 1 screw terminal			
mechanical data  width * height * depth of the enclosure  installation with x mounting height  125 × 225 mm  126 × 225 mm  stallation with x mounting height  126 × 225 mm  50 mm  • bottom  • left  0 mm  • left  0 mm  50 mm  • left  • dight  • standard rail mounting  • x vail mounting  No  • vail mounting  No  • wall mounting  No  housing can be lined up  Yes  mechanical accessories  mechanical accessories  mechanical accessories  provides industry Mail  • to website: Industry Chiline Support  additional information  other information  Security information  Classifications and accessors are used. Use of product versions that are no longer sentence industry are approached and the support the secure operation of plants, systems, machines and revolves in necessary and only when appropriate security information on the secure operation of plants, systems, machines and revolves in necessary and only when appropriate security personal points are not products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and revolves in necessary to implement – and continuously mariain – a holistic state-of-the-art industrial cybersecurity compensations on revolves in necessary and only when appropriate security measures (e.g. firewills and on plants) in the secure operation of plants, systems, machines and revolves in necessary and only when appropriate security measures (e.g. firewills and on plants) in the secure operation of plants, systems, machines and revolves in necessary and only when appropriate security measures (e.g. firewills and on networise on elements of such a concept. Classomers are responsible and	suitability for interaction modular system	Yes	Yes			
width × height × depth of the enclosure installation width × mounting height  128 × 228 mm  128 × 22	type of connection to system components	Via integrated connector				
Installation width × mounting height  128 × 228 mm  required spacing  • top  • bothom  • bothom  • left  • left  • omm  • stright  Omm  • stright  Omm  • stright  • standard rall mounting  • S7 rall mounting  • S7 rall mounting  • wall mounting  • to websate: industry Mall  • to websate: industry Online Support  • that "Namport industry stemens com  statical information  • that "Namport industry stemens comitions with industrial cybersecurity functions that support industry stemens com  statical information  • that "Namport industry stemens com  statical information  • that "Namport industry stemens com  statical information  • that "Namport industr	mechanical data					
required specing  • top  • bottom  • left  • oright  fastening method  • standard rail mounting  • wall mounting  • to website: industry Mall  • to website: industry Mall  • to website: industrial communication  • to website: industrial communication  • to website: industrial communication  • to website: industry Online Support  • to website: industrial communication  • to website: industry Online Support  • to website: industrial communication	width × height × depth of the enclosure	125 × 125 × 150 mm				
• lop     • bottom     • left     • injet     • injet     • injet     • injet     • standard rail mounting     • standard rail mounting     • standard rail mounting     • S7 rail mounting     • No     • well mounting     No     housing can be lined up     net weight     increasories     mechanical accessories     mechanical accessories     mechanical accessories     mechanical accessories     mechanical accessories     mechanical accessories     internet link     • to website: industry Mall     • to website: industry Mall     • to website: industry Mall     • to website: industry Online Support     • to website: industry Online Support     additional information     • to website: industry Online Support     additional information     other information     security information information information infor	installation width × mounting height	125 × 225 mm				
bottom   left   0 mm	required spacing					
e left o might o mm origin webod   standard rail mounting	• top	50 mm				
e right fastening method	• bottom	50 mm	50 mm			
fastening method  • standard rail mounting • syr all mounting • wall mounting • to least the standard of the s	<ul><li>left</li></ul>	0 mm	0 mm			
Standard rail mounting     ST rail mounting     No     wall mounting     No     housing can be lined up     ret weight     1,95 kg  ### ### ### ### ### ### ### ### ### #			0 mm			
Solution and the lined up point weight probability and the line of the line o		·	Snaps onto DIN rail EN 60715 35x15			
No wall mounting     No yes     Internet link	-					
housing can be lined up  net weight  1.95 kg  sccessories  mechanical accessories  mechanical accessories  purcher information internet links  internet link  • to website: Industriy Mall  • to website: Industrial communication  • to website: Industrial communication  • to website: CAx-Download-Manager  • to website: Industry Online Support  additional information  other information  Specifications at rated input voltage and ambient temperature 425 °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. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and centernial order threats, it is necessary to implement—and confinuously maritan—a holistic, state-of-the-art industrial cybersecurity concept. Stemens provides and solutions constitute one element of such a concept. Customers are responsible for threats, it is necessary to the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connected to an enterprise network or the internet if and to the extent such a connection in necessary and only when appropriate security measures (e.g. firevalls and/or network segmentation) are place. For antients 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 are used. Use of product versions are used of the product versions are used. Use of product versions are such material to the security machines and complete such as a conscious of the product versions are used. Use of product versions a	S7 rail mounting					
net weight  accessories  mechanical accessories  further information internet links  internet link  • to website: Industry Mall  • to website: Industrial communication  • to website: Accessories  to website: Accessories  to website: Industrial communication  • to website: Accessories  to website: Industry Online Support  activity information  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 implement—and continuously maintain—a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of seuta eleme	wall mounting		No			
mechanical accessories  Device identification label 20 mm × 7 mm, TI-grey 3RT2900-1SB20  further information internet links  internet link  • to website: industry Mall  • to website: industry Mall  • to website: industrial communication  • to website: industrial communication  • to website: industrial communication  • to website: industry Online Support  • to website: industry Online  • to website:	·					
mechanical accessories  further information internet links  internet link  • to website: Industry Mall  • to website: Industrial communication  • to website: CAx-Download-Manager  • to website: Industry Online Support  • to website: Industry Online Support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement a connect on solutions on the Industrial on the Industrial operation on Indust		1.95 kg				
internet link  internet link  it to website: Industry Mall  it to web page: selection aid TIA Selection Tool  it to website: Industrial communication  it to website: Industrial communication  it to website: Industry Online Support  It to website:	accessories					
Internet link  • to website: Industry Mall  • to website: Industrial communication  • to website: Industrial communication  • to website: CAx-Download-Manager  • to website: Industry Online Support  additional information  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 i 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 undustry. Simems i 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 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 these or 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 say informed about product updates, subscribe to		Device identification label 20 m	m × 7 mm, TI-grey 3RT29	900-1SB20		
to website: Industry Mall     to web page: selection aid TIA Selection Tool     to website: Industrial communication     to website: CAx-Download-Manager     to website: Industry Online Support     additional information  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  security information  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 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 patients from a time of 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)  Classifications						
to web page: selection aid TIA Selection Tool     to website: Industrial communication     to website: CAx-Download-Manager     to website: Industry Online Support     dadditional 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 in order to protect plants, systems, machines and networks sale-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 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 treats on sa they are available and that the latest product treats on sa they are available and that the latest product treats on sa they are available and that the latest product treats on sa they are available and that the latest product treats on sa they are available and that the latest product treats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)  Classifications						
to website: Industrial communication to website: CAx-Download-Manager to website: CAx-Download-Manager thitps://siemens.com/cax thtps://siemens.com/cax thtps://siemens.com/c	-					
to website: CAx-Download-Manager to website: Industry Online Support  https://support.industry.siemens.com  didditional 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 and solutions constitute ne element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and 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/cybersecurity informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cybersecurity RSS Feed under						
• to website: Industry Online Support  additional information  other information  Specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)  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, and 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)  Classifications  Version Classification  eClass 14 27-04-07-05 eClass  eClass 9.1 27-04-07-05						
additional 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 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)  Classifications  Classification  eClass 14 27-04-07-05 eClass eClass 9.1 27-04-07-05	_					
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 deplopment 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)  Classifications  Version Classification  eClass 14 27-04-07-05 eClass 12 27-04-07-05 eClass 9.1 27-04-07-05		nttps://support.industry.siemens	https://support.industry.siemens.com			
security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and 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 (page firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (page sevisit 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)  Classifications  Classification  eClass 14 27-04-07-05 eClass eClass 9.1 27-04-07-05						
Security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and 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)  Classifications  Classification  eClass 14 27-04-07-05 eClass 12 27-04-07-05 eClass 9.1 27-04-07-05	other information		tage and ambient temper	rature +25 °C (unless		
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)  Classification  Classification  eClass  14  27-04-07-05  eClass  9.1  27-04-07-05	security information	omermes speames,				
that support the secure operation of plants, systems, machines and networks all norder 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)  Classifications  Classification  eClass 14 27-04-07-05  eClass 12 27-04-07-05  eClass 9.1 27-04-07-05	· · · · · · · · · · · · · · · · · · ·	Siemens provides products and	I solutions with industrial	cyhersecurity functions		
Version         Classification           eClass         14         27-04-07-05           eClass         12         27-04-07-05           eClass         9.1         27-04-07-05		In order to protect plants, syste threats, it is necessary to imple state-of-the-art industrial cybers solutions constitute one elemen for preventing unauthorized acc networks. Such systems, mach to an enterprise network or the necessary and only when appronetwork segmentation) are in picybersecurity measures that may www.siemens.com/cybersecurity undergo continuous developmentecommends that product upday and that the latest product version longer supported, and failure customer's exposure to cyber the subscribe to the Siemens Industrial	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			
eClass 14 27-04-07-05 eClass 12 27-04-07-05 eClass 9.1 27-04-07-05	Classifications					
eClass 12 27-04-07-05 eClass 9.1 27-04-07-05			Version	Classification		
eClass 9.1 27-04-07-05		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** 





Manufacturer Declaration Declaration of Conformity





## Marine / Shipping





last modified: 6/24/2024 🖸