# SIEMENS

## Data sheet

## 6EP1437-2BA20



SITOP PSU300S/3AC/24VDC/40A

SITOP PSU300S 40 A stabilized power supply input: 400-500 V 3 AC output: 24 V DC/40 A

input			
type of the power supply network	3-phase AC		
supply voltage at AC			
minimum rated value	400 V		
maximum rated value	500 V		
• initial value	340 V		
• full-scale value	550 V		
wide range input	Yes		
buffering time for rated value of the output current in the event of power failure minimum	6 ms		
operating condition of the mains buffering	at Vin = 400 V		
line frequency	50/60 Hz		
line frequency	47 63 Hz		
input current			
<ul> <li>at rated input voltage 400 V</li> </ul>	2 A		
<ul> <li>at rated input voltage 500 V</li> </ul>	1.7 A		
current limitation of inrush current at 25 °C maximum	60 A		
I2t value maximum	3.4 A <sup>2</sup> ·s		
fuse protection type	none		
fuse protection type in the feeder	Required: 3-pole connected miniature circuit breaker 10 16 A characteristic C or circuit breaker 3RV2011-1DA10 (setting 3 A) or 3RV2711-1DD10 (UL 489-listed, DIVQ)		
output			
voltage curve at output	Controlled, isolated DC voltage		
output voltage at DC rated value	24 V		
output voltage			
<ul> <li>at output 1 at DC rated value</li> </ul>	24 V		
output voltage adjustable	Yes; via potentiometer		
adjustable output voltage	24 28 V; max. 960 W		
relative overall tolerance of the voltage	3 %		
relative control precision of the output voltage			
on slow fluctuation of input voltage	1 %		
<ul> <li>on slow fluctuation of ohm loading</li> </ul>	2 %		
residual ripple			
• maximum	150 mV		
voltage peak			
• maximum	240 mV		
display version for normal operation	Green LED for 24 V OK		
	Green LLD 101 24 V OK		
type of signal at output	Relay contact (NO contact, rating 60 V DC/ 0.3 A) for "24 V OK"		

voltage increase time of the output voltage	
voltage increase time of the output voltage	15 ms
• typical • maximum	15 ms 500 ms
	500 ms
output current	40 A
rated value	
rated range	0 40 A; 48 A up to +45°C; +60 +70 °C: Derating 3%/K
supplied active power typical	960 W
short-term overload current	
<ul> <li>on short-circuiting during the start-up typical</li> </ul>	65 A
at short-circuit during operation typical	65 A
duration of overloading capability for excess current	
<ul> <li>on short-circuiting during the start-up</li> </ul>	100 ms
at short-circuit during operation	100 ms
bridging of equipment	Yes
number of parallel-switched equipment resources for increasing the power	2
efficiency	
efficiency in percent	91.5 %
power loss [W]	
at rated output voltage for rated value of the output	89 W
current typical	
closed-loop control	
relative control precision of the output voltage with rapid fluctuation of the input voltage by +/- 15% typical	3 %
relative control precision of the output voltage load step of resistive load 50/100/50 % typical	1.5 %
setting time	
<ul> <li>load step 50 to 100% typical</li> </ul>	1 ms
<ul> <li>load step 100 to 50% typical</li> </ul>	1 ms
relative control precision of the output voltage at load step of resistive load 10/90/10 % typical	3 %
setting time	
<ul> <li>load step 10 to 90% typical</li> </ul>	1 ms
<ul> <li>load step 90 to 10% typical</li> </ul>	1 ms
• maximum	10 ms
protection and monitoring	
design of the overvoltage protection	protection against overvoltage in case of internal fault Vout < 35 V
property of the output short-circuit proof	Yes
design of short-circuit protection	Electronic shutdown, automatic restart
typical	50 A
overcurrent overload capability	
in normal operation	overload capability 150 % lout rated up to 5 s/min
enduring short circuit current RMS value	
• maximum	14 A
safety	
galvanic isolation between input and output galvanic isolation	Yes Safety extra-low output voltage Vout acc. to EN 60950-1 and EN 50178, transformer age to EN 64558 2.16
operating recourse protection along	transformer acc. to EN 61558-2-16
operating resource protection class	
protection class IP	IP20
EMC	
standard	EN 55022 Class P
<ul> <li>for emitted interference</li> <li>for mains harmonics limitation</li> </ul>	EN 55022 Class B
for interference immunity	EN 61000-3-2 EN 61000-6-2
• for interference immunity standards, specifications, approvals	
certificate of suitability	Yes
CE marking	Yes Yes; cULus-Listed (UL 508, CSA C22.2 No. 107.1), File E197259; cCSAus
UL approval	(CSA C22.2 No. 60950-1, UL 60950-1)
CSA approval	Yes; cULus-Listed (UL 508, CSA C22.2 No. 107.1), File E197259; cCSAus (CSA C22.2 No. 60950-1, UL 60950-1)

	Y.
UKCA marking	Yes
EAC approval	Yes
NEC Class 2	No
type of certification	
• BIS	Yes; R-41183539
CB-certificate	Yes
MTBF at 40 °C	500 000 h
standards, specifications, approvals hazardous environments	
certificate of suitability	
• IECEx	No
• ATEX	No
ULhazloc approval	No
<ul> <li>cCSAus, Class 1, Division 2</li> </ul>	No
FM registration	No
standards, specifications, approvals marine classification	
shipbuilding approval	Yes
Marine classification association	
American Bureau of Shipping Europe Ltd. (ABS)	Yes
French marine classification society (BV)	No
Det Norske Veritas (DNV)	Yes
Lloyds Register of Shipping (LRS)	No
standards, specifications, approvals Environmental Product Dec	
Standards, specifications, approvals Environmental Product Det Environmental Product Declaration	
	Yes
global warming potential [CO2 eq]	0.0471
• total	2 847 kg
during manufacturing	61.2 kg
during operation	2 783.6 kg
after end of life	0.92 kg
ambient conditions	
ambient temperature	
during operation	-25 +70; with natural convection
<ul> <li>during transport</li> </ul>	-40 +85
during storage	-40 +85
environmental category according to IEC 60721	Climate class 3K3, 5 95% no condensation
connection method	
type of electrical connection	screw terminal
• at input	L1, L2, L3, PE: 1 screw terminal each for 0.5 4 mm <sup>2</sup> single-core/finely stranded
● at output	+, -: 2 screw terminals each for 0.5 10 mm <sup>2</sup>
<ul> <li>for auxiliary contacts</li> </ul>	13, 14 (alarm signal): 1 screw terminal each for 0.05 2.5 mm <sup>2</sup>
mechanical data	
width × height × depth of the enclosure	145 × 145 × 150 mm
installation width × mounting height	145 mm × 225 mm
required spacing	
• top	40 mm
• bottom	40 mm
● left	0 mm
● right	0 mm
fastening method	Snaps onto DIN rail EN 60715 35x15
DIN-rail mounting	Yes
S7 rail mounting	No
wall mounting	No
housing can be lined up	Yes
net weight	3.1 kg
accessories	
	Podundanau modulo, huffor modulo, polasti itu modulo, DO UDO
electrical accessories	Redundancy module, buffer module, selectivity module, DC UPS
mechanical accessories	Device identification label 20 mm × 7 mm, pale turquoise 3RT1900-1SB20
further information internet links	
internet link	
• to website: Industry Mall	https://mall.industry.siemens.com

• to web page: selection aid TIA Selection Tool       https://www.siemens.com/sitoput         • to web page: power supplies       https://siemens.com/sitoput         • to website: CAx-Download-Manager       https://siemens.com/cax         • to website: Industry Online Support       https://siemens.com         additional information       specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)         security 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 adjust cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity measures should only be connected 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. Such systems, machines and componented, please wist www.siemens.com/cybersecurity. Siemens 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 and industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in plac	• to web page: power supplies       https://siemens.com/sitop         • to website: CAx-Download-Manager       https://siemens.com/cax         • to website: Industry Online Support       https://siemens.com/cax         additional information       additional information         security 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 against cyber recently measures that may be implemented, please visit www. siemens.com/cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www. siemens.com/cybersecurity measures that may be implemented, please visit www. siemens.com/cybersecurity measures that as olutions 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 sens strongly recommends that product updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cyberesecurity RSS Feed under		
• to website: CAx-Download-Manager       https://siemens.com/cax         • to website: Industry Online Support       https://support.industry.siemens.com         additional information       specifications at rated input voltage and ambient temperature +25 °C (unless otherwise specified)         security 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 holisic, 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 only be connected to an enterprise network or the internet if and to the extent such a contection is necessary and only when appropriate security siemes (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity endustry. 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, subscribe to the Siemens Industrial Cybersecurity RSS Feed under	• to website: CAx-Download-Manager       https://siemens.com/cax         • to website: Industry Online Support       https://support.industry.siemens.com         additional 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. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. Such solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and 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. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly www.siemens.com/cybersecurity.siemens (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity endustry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly are obmers 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	<ul> <li>to web page: selection aid TIA Selection Tool</li> </ul>	https://www.siemens.com/tstcloud
• to website: Industry Online Support       https://support.industry.siemens.com         additional 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 saginst 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 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-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	• to website: Industry Online Support       https://support.industry.siemens.com         additional 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. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks segmentation in ceessary and only when appropriate security one extent so the acconcept of the ast of the art industrial cybersecurity industrial cybersecurits and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks segmentation) are in place. For additional information on industrial cybersecurity one sures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity concept on 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 is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity concept continuous development to make them more secure. Siemens strongly 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 upd	<ul> <li>to web page: power supplies</li> </ul>	https://siemens.com/sitop
additional 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. Clastomers 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-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	additional 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	<ul> <li>to website: CAx-Download-Manager</li> </ul>	https://siemens.com/cax
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 onetworks. Such systems, machines and onetwork segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-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	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 onponents 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 RS Feed under	<ul> <li>to website: Industry Online Support</li> </ul>	https://support.industry.siemens.com
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 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	security information Security	additional 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 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	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 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	other 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	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	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

### Classifications

	Version	Classification
eClass	14	27-04-07-01
eClass	12	27-04-07-01
eClass	9.1	27-04-07-01
eClass	9	27-04-07-01
eClass	8	27-04-90-02
eClass	7.1	27-04-90-02
eClass	6	27-04-90-02
ETIM	9	EC002540
ETIM	8	EC002540
ETIM	7	EC002540
IDEA	4	4130
UNSPSC	15	39-12-10-04

### Approvals Certificates

#### General Product Approval

СВ	(Sp)	<u>Manufacturer Declara-</u> <u>tion</u>	Declaration of Con- formity	UK CA	CE EG-Konf.
General Product Appro	oval	Marine / Shipping		Environment	
	<u>BIS CRS</u>	ABS		EPD	
last modified:		11/25	/2024 🖸		