

product type designation



Aluminum housing with protection class IP68

Degree of protection of aluminum enclosure IP68; suitable for SIMATIC RTU3000C; temperature range -40 to +80 °C; Cover with pin-torx screws; 7 Cable bushings and bushing for mobile radio antenna prepared; please order the cable glands and sealing plugs in the required number separately .

suitability for use	Degree of protection IP68 1 m / 24 h
suitability for operation	suitable for devices of the SIMATIC RTU3000C range
mechanical data	
material	aluminum, powder coated
color	gray (RAL 7001)
ambient conditions	
ambient temperature	
• during operation	-40 ... +80 °C
• during storage	-40 ... +80 °C
• during transport	-40 ... +80 °C
relative humidity	
• at 30 °C / without condensation / during operation / maximum	95 %
protection class IP	IP68; 1 m / 24 h, observe the installation instructions
design, dimensions and weights	
width	280 mm
height	230 mm
depth	111 mm
net weight	3395 g
design of the screw head / torx	Yes; Pin-Torx
installation or assembly note	Required tightening torques: Cable gland with article number 6NH3112-3BA00-1XX4: Cap nut 5 - 6 Nm, fittings 3.5 - 4.5 Nm, sealing plug with the article number 6NH3112-3BA00-1XX5: 2.5 - 3.5 Nm
standards, specifications, approvals	
reference code	
• according to IEC 81346-2:2019	CMB
further information / internet links	
internet link	
• to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
• to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
• to website: Industrial communication	https://www.siemens.com/simatic-net
• to web page: SiePortal	https://sieportal.siemens.com/
• to website: Image database	https://www.automation.siemens.com/bilddb
• to website: CAX-Download-Manager	https://www.siemens.com/cax
• to website: Industry Online Support	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)

last modified:

1/28/2025 