

product brand name	RUGGEDCOM
product type designation	RX1500PN LM APE1402
	**** Replacement part **** RUGGEDCOM RX1500PN LM APE1402 Line Module Application Processing Engine, 1.3Ghz, 2GB RAM, 8GB SSD, Linux

hardware configuration

processor clock frequency	1.3 GHz
design of the drive/storage medium / solid-state disk	Yes
storage capacity / on hard disk	8 Gabyte
storage capacity / of the RAM	2 Gabyte
operating system / pre-installed	Linux

design, dimensions and weights

product feature / conformal coating	No
-------------------------------------	----

further information / internet links

internet link	
<ul style="list-style-type: none"> to website: Selection guide for cables and connectors to website: Industry Mall/RUGGEDCOM selector to website: Industrial communication to website: Siemens RUGGEDCOM to website: Image database to website: CAX-Download-Manager to website: Industry Online Support 	https://support.industry.siemens.com/cs/ww/en/view/109766358 https://ruggedcom-selector.automation.siemens.com/ https://www.siemens.com/simatic-net https://siemens.com/ruggedcom https://www.automation.siemens.com/bilddb https://www.siemens.com/cax https://support.industry.siemens.com

security information

security information	<p>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)</p>
----------------------	---

Approvals / Certificates

General Product Approval	other	Dangerous goods	Environment
Manufacturer Declaration 	 EG-Konf.	inspection certificate Dangerous goods information	

last modified: 3/18/2025 