SIEMENS

Data sheet 6GK6015-0AL20-0GF0

product brand name	RUGGEDCOM
product type designation	RX1500PN LM APE1404CKP
	**** Replacement part **** RUGGEDCOM RX1500PN LM APE1404CKP Line Module Application Processing Engine 1.3GHz, 2GB RAM, 16GB SATA, DVI-D Video, 2xUSB, Checkpoint FW (Requires Checkpoint License)
product brand name	RUGGEDCOM
hardware configuration	
processor clock frequency	1.3 GHz
storage capacity / on hard disk	16 Gibyte; SATA
storage capacity / of the RAM	2 Gibyte
operating system / pre-installed	Checkpoint FW (Requires Checkpoint License)
design, dimensions and weights	
product feature / conformal coating	No
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 website: Industry Mall/RUGGEDCOM selector	https://ruggedcom-selector.automation.siemens.com/
• to website: Industrial communication	https://www.siemens.com/simatic-net
• to website: Siemens RUGGEDCOM	https://siemens.com/ruggedcom
• 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)

Approvals / Certificates

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

last modified: 3/10/2026

Subject to change without notice
© Copyright Siemens