SIEMENS

Data sheet 6GK6095-0GS11-0BA0

	**** Replacement part **** RUGGEDCOM RS950GNC is an industrially hardened PRP/HSR redundancy box (RedBox) with 56-bit Encryption providing 3 Gigabit Ethernet combo ports (100FX/1000LX/1000 SX or 10/100/1000TX), 2 HSR/PRP redundant ports and 1 regular access port (SAN) for standard Ethernet devices 24 = 24 VDC (10-36 VDC) No power supply 2 D = DIN Rail Mounting . XX = Manufacturing modification: none
product type designation	
product brand name	RUGGEDCOM
product type designation	RS950GNC
transfer rate	
transfer rate	100 Mbit/s, 1000
interfaces / other	
number of electrical connections	
● for operator console	1
type of electrical connection	
● for operator console	RS232
● for signaling contact	3-pole terminal block, can be screwed
● for power supply	5-pole terminal block, screwable
supply voltage, current consumption, power loss	
type of voltage / 1 / of the supply voltage	DC
● supply voltage / 1 / rated value	24 V
● power loss [W] / 1 / rated value	10 W
● consumed current / 1 / at rated supply voltage / maximum	1.2 A
type of voltage / 2 / of the supply voltage	DC
● supply voltage / 2 / rated value	48 V
● consumed current / 2 / at rated supply voltage / maximum	0.6 A
ambient conditions	
ambient temperature	
● during operation	-40 ... +85 °C
● note	A maximum operating temperature of +85 °C is permissible for a duration of 16 hours
operating condition / fanless operation	Yes
protection class IP	IP40
design, dimensions and weights	
design	compact
width	65.02 mm
height	188 mm
depth	116.59 mm
net weight	1.22 kg
material / of the enclosure	20 AWG galvanized steel enclosure
fastening method	
● 19-inch installation	No
● 35 mm DIN-rail mounting	Yes
● wall mounting	Yes
product features, product functions, product components / general	
number of automatically learnable MAC addresses	1024
product functions / management, configuration, engineering	
product function	
● CLI	Yes
● web-based management	Yes
● MIB support	Yes
● RMON	Yes

Subject to change without notice
© Copyright Siemens

● switch-managed	Yes
protocol / is supported	
● Telnet	Yes
● HTTP	Yes
● HTTPS	Yes
● TFTP	Yes
● SNMP v1	Yes
● SNMP v2	No
● SNMP v3	Yes
● IGMP (snooping/querier)	No
product functions / DHCP	
product function	
● DHCP client	Yes
● DHCP Option 82	No
● DHCP Option 66	No
● DHCP Option 67	No
product functions / redundancy	
product function	
● High-availability Seamless Redundancy (HSR)	Yes
● Parallel Redundancy Protocol (PRP)/operation in the PRP-network	Yes
● Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA)	Yes
protocol / is supported	
● STP	Yes
● RSTP	Yes
● MSTP	Yes
product functions / security	
protocol / is supported	
● RADIUS	Yes
product functions / time	
product function	
● SNTP client	Yes
● IEEE 1588 v2 transparent forwarding	Yes
protocol / is supported	
● SNTP	Yes
standards, specifications, approvals	
certificate of suitability	
● CE marking	Yes
standard	
● for EMC	FCC Part 15 (Class A), EN55022 (CISPR22 Class A)
● for safety / from CSA and UL	cCSAus (Compliant with CSA C22.2 No. 60950, UL60950, EN60950)
standards, specifications, approvals / other	
certificate of suitability	
● IEC 61850-3	Yes
product functions / general	
laser protection class	21 CFR Chapter 1, Subchapter J
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: Industrial communication	https://www.siemens.com/simatic-net
● 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

© Copyright Siemens

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

Environment	General Product Approval				
EPD	Manufacturer Declaration	CE EG-Konf.	UKCA	RCM	Declaration of Conformity

Functional Saftey		Test Certificates		other	Dangerous goods
CSA	UL	CB	Type Test Certificates/Test Report	inspection certificate	Dangerous goods information

last modified: 6/12/2026

Subject to change without notice
© Copyright Siemens