



SCALANCE X204RNA; redundant network access; 4x 100 Mbit/s RJ45 ports; LED diagnostics; error-signaling contact with set push-button; redundant power supply; network management; including electronic manual on CD-ROM, C-PLUG optional for HSR networks;

product type designation	
product brand name	SCALANCE
product type designation	X204RNA
Technical Product Detail Page	<a href="https://i.siemens.com/1P6GK5204-0BA00-2MB2">https://i.siemens.com/1P6GK5204-0BA00-2MB2</a>
transfer rate	
transfer rate	10, 100 Mbit/s
interfaces / for communication / integrated	
number of electrical connections	
• for network components or terminal equipment	4
interfaces / other	
number of electrical connections	
• for signaling contact	1
• for power supply	1
design of the removable storage	
• C-PLUG	Yes
operating voltage / of the signaling contacts	
• at DC / rated value	24 V
operational current / of the signaling contacts	
• at DC / maximum	0.1 A
supply voltage, current consumption, power loss	
product component / connection for redundant voltage supply	Yes
<b>type of voltage / 1 / of the supply voltage</b>	
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	3.5 W
• supply voltage / 1 / voltage range	19.2 ... 28.8
• consumed current / 1 / maximum	0.15 A
• product component / 1 / fusing at power supply input	Yes
ambient conditions	
ambient temperature	
• during operation	-40 ... +60 °C
• during storage	-40 ... +70 °C
• during transport	-40 ... +70 °C
relative humidity	
• at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP20
design, dimensions and weights	
design	compact
width	45 mm

height	100 mm
depth	87 mm
net weight	0.23 kg
fastening method	
• 35 mm DIN-rail mounting	Yes
• wall mounting	Yes
• S7-300 rail mounting	No
• S7-1500 rail mounting	No

**product functions / management, configuration, engineering**

product function	
• CLI	Yes
• web-based management	Yes
• MIB support	Yes
• TRAPs via email	Yes
• configuration with STEP 7	No
• port mirroring	No
• multipoint mirroring	No
• with IRT / PROFINET IO switch	No
• PROFINET IO diagnosis	No
• switch-managed	No
protocol / is supported	
• Telnet	No
• HTTP	Yes
• HTTPS	Yes
• TFTP	No
• FTP	No
• BOOTP	No
• GMRP	No
• DCP	Yes
• LLDP	No
• SNMP v1	Yes
• SNMP v2	Yes
• SNMP v3	Yes
• IGMP (snooping/querier)	No
identification & maintenance function	
• I&M0 - device-specific information	Yes
• I&M1 - higher level designation/location designation	Yes

**product functions / diagnostics**

product function	
• port diagnostics	Yes
• statistics Packet Size	Yes
• statistics packet type	Yes
• error statistics	Yes

**product functions / redundancy**

protocol / is supported / Media Redundancy Protocol (MRP)	No
product function	
• media redundancy protocol (MRP) with redundancy manager	No
• ring redundancy	Yes
• high speed redundancy protocol (HRP) with redundancy manager	No
• high speed redundancy protocol (HRP) with standby redundancy	No
• High-availability Seamless Redundancy (HSR)	Yes
• Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA)	Yes
• High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) coupling	No
• passive listening	No

**product functions / security**

protocol / is supported	
<ul style="list-style-type: none"> <li>• SSH</li> </ul>	Yes
<b>product functions / time</b>	
product function	
<ul style="list-style-type: none"> <li>• SICLOCK support</li> </ul>	No
protocol / is supported	
<ul style="list-style-type: none"> <li>• NTP</li> <li>• Sntp</li> </ul>	No Yes
<b>standards, specifications, approvals</b>	
certificate of suitability	
<ul style="list-style-type: none"> <li>• CE marking</li> <li>• KC approval</li> <li>• Regulatory Compliance Mark (RCM)</li> </ul>	Yes Yes Yes
standard	
<ul style="list-style-type: none"> <li>• for EMC interference emission</li> <li>• for immunity to EMC</li> <li>• for safety / from CSA and UL</li> </ul>	EN 61000-6-4:2001 (Class A) EN 61000-6-4:2001 UL 60950-1 E115352, CSA C22.2 No. 60950-1
<b>standards, specifications, approvals / hazardous environments</b>	
certificate of suitability	
<ul style="list-style-type: none"> <li>• ATEX</li> <li>• UKEX</li> <li>• IECEx</li> <li>• CCC / for hazardous zone according to GB standard</li> <li>• FM registration</li> </ul>	Yes Yes Yes Yes Yes
<b>standards, specifications, approvals / other</b>	
certificate of suitability	
<ul style="list-style-type: none"> <li>• railway application in accordance with EN 50155</li> <li>• railway application in accordance with EN 50124-1</li> <li>• IEC 61850-3</li> <li>• RoHS conformity</li> </ul>	No No No Yes
<b>product functions / general</b>	
MTBF	92.45 a
warranty period	5 a
product function / is supported / identification link	Yes; acc. to IEC 61406-1:2022
<b>further information / internet links</b>	
internet link	
<ul style="list-style-type: none"> <li>• to website: Selection guide for cables and connectors</li> <li>• to web page: selection aid TIA Selection Tool</li> <li>• to website: Industrial communication</li> <li>• to web page: SiePortal</li> <li>• to website: Image database</li> <li>• to website: CAX-Download-Manager</li> <li>• to website: Industry Online Support</li> </ul>	<a href="https://support.industry.siemens.com/cs/ww/en/view/109766358">https://support.industry.siemens.com/cs/ww/en/view/109766358</a> <a href="https://www.siemens.com/tstcloud">https://www.siemens.com/tstcloud</a> <a href="https://www.siemens.com/simatic-net">https://www.siemens.com/simatic-net</a> <a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a> <a href="https://www.automation.siemens.com/bilddb">https://www.automation.siemens.com/bilddb</a> <a href="https://www.siemens.com/cax">https://www.siemens.com/cax</a> <a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
<b>security information</b>	
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 <a href="http://www.siemens.com/cybersecurity-industry">www.siemens.com/cybersecurity-industry</a>. 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 <a href="https://www.siemens.com/cert">https://www.siemens.com/cert</a>. (V4.7)</p>

Approvals / Certificates

General Product Approval



[Declaration of Conformity](#)



[China RoHS](#)

[Miscellaneous](#)

General Product Approval

EMV

For use in hazardous locations



[KC](#)



IECEX



[EM](#)

[CCC-Ex](#)

Maritime application



last modified:

10/30/2025 