

SCALANCE XR324WG; managed IE switch; 19" rack; 24 x 10/100 Mbit/s electrical ports; LED diagnostics; reset button; console port; PROFINET device; IEC 62443-4-2 certified network management function; redundancy manager; power supply 24 V DC;



product type designation	
product brand name	SCALANCE
product type designation	XR324 WG
Technical Product Detail Page	<a href="https://i.siemens.com/1P6GK5324-0BA00-2AR3">https://i.siemens.com/1P6GK5324-0BA00-2AR3</a>
transfer rate	
transfer rate	10, 100 Mbit/s
interfaces / for communication / integrated	
number of electrical connections	
• for network components or terminal equipment	24; RJ45
number of 10/100 Mbit/s RJ45 ports	24
interfaces / other	
number of electrical connections	
• for operator console	1
• for power supply	1
supply voltage, current consumption, power loss	
type of voltage supply / redundant power supply unit	No
<b>type of voltage / 1 / of the supply voltage</b>	
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	7.2 W
• supply voltage / 1 / voltage range	19.2 ... 28.8
• consumed current / 1 / maximum	0.3 A
• product component / 1 / fusing at power supply input	Yes
ambient conditions	
ambient temperature	
• during operation	0 ... 60 °C
• during storage	-40 ... +85 °C
• during transport	-40 ... +85 °C
relative humidity	
• at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP30
design, dimensions and weights	
design	19-inch rack
number of modular height units / relating to 19-inch cabinet	1
width	483 mm
height	44 mm
depth	127 mm
net weight	2.7 kg
fastening method	

<ul style="list-style-type: none"> <li>• 19-inch installation</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• 35 mm DIN-rail mounting</li> </ul>	No
<ul style="list-style-type: none"> <li>• wall mounting</li> </ul>	No
<ul style="list-style-type: none"> <li>• S7-300 rail mounting</li> </ul>	No
<ul style="list-style-type: none"> <li>• S7-1500 rail mounting</li> </ul>	No
<b>product features, product functions, product components / general</b>	
cascading in the case of a redundant ring / at reconfiguration time of <math>\leq 0.3\text{ s}</math>	50
cascading in cases of star topology	any (depending only on signal propagation time)
<b>product functions / management, configuration, engineering</b>	
product function	
<ul style="list-style-type: none"> <li>• CLI</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• web-based management</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• MIB support</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• TRAPs via email</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• configuration with STEP 7</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• RMON</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• port mirroring</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• multiport mirroring</li> </ul>	No
<ul style="list-style-type: none"> <li>• CoS</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• PROFINET IO diagnosis</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• switch-managed</li> </ul>	Yes
PROFINET conformity class	B
network load class / according to PROFINET	II
protocol / is supported	
<ul style="list-style-type: none"> <li>• Telnet</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• HTTP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• HTTPS</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• TFTP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• FTP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• BOOTP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• GMRP</li> </ul>	No
<ul style="list-style-type: none"> <li>• DCP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• LLDP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• SNMP v1</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• SNMP v2</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• SNMP v3</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• IGMP (snooping/querier)</li> </ul>	Yes
identification & maintenance function	
<ul style="list-style-type: none"> <li>• I&amp;M0 - device-specific information</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• I&amp;M1 - higher level designation/location designation</li> </ul>	Yes
<b>product functions / diagnostics</b>	
product function	
<ul style="list-style-type: none"> <li>• port diagnostics</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• statistics Packet Size</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• statistics packet type</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• error statistics</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• SysLog</li> </ul>	Yes
<b>product functions / VLAN</b>	
product function	
<ul style="list-style-type: none"> <li>• VLAN - port based</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• VLAN - protocol-based</li> </ul>	No
<ul style="list-style-type: none"> <li>• VLAN - IP-based</li> </ul>	No
<ul style="list-style-type: none"> <li>• VLAN dynamic</li> </ul>	Yes
number of VLANs / maximum	257
number of VLANs - dynamic / maximum	257
number of VLANs / at ring redundancy (HRP; MRP; standby link)	257
<b>product functions / DHCP</b>	

product function	
• DHCP client	Yes
• DHCP Option 82	Yes
• DHCP Option 66	Yes
• DHCP Option 67	Yes
<b>product functions / redundancy</b>	
protocol / is supported / Media Redundancy Protocol (MRP)	Yes
product function	
• media redundancy protocol (MRP) with redundancy manager	Yes
• ring redundancy	Yes
• high speed redundancy protocol (HRP) with redundancy manager	Yes
• high speed redundancy protocol (HRP) with standby redundancy	Yes
• redundancy procedure STP	Yes
• redundancy procedure RSTP	Yes
• redundancy procedure MSTP	No
• Parallel Redundancy Protocol (PRP)/operation in the PRP-network	Yes
• Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA)	No
• passive listening	Yes
protocol / is supported	
• STP/RSTP	Yes
• STP	Yes
• RSTP	Yes
• MSTP	No
• RSTP big network support	Yes
• LACP	No
<b>product functions / security</b>	
product function	
• IEEE 802.1x (radius)	Yes
• broadcast/multicast/unicast limiter	Yes
• broadcast blocking	Yes
protocol / is supported	
• SSH	Yes
<b>product functions / time</b>	
product function	
• SICLOCK support	Yes
protocol / is supported	
• NTP	Yes
• SNTP	Yes
• IEEE 1588 profile default	No
<b>standards, specifications, approvals</b>	
certificate of suitability	
• CE marking	Yes
• UKCA marking	Yes
• KC approval	Yes
• Regulatory Compliance Mark (RCM)	Yes
standard	
• for EMC interference emission	EN 61000-6-4 (Class B)
• for immunity to EMC	EN 61000-6-2
• for safety / from CSA and UL	UL 60950-1, CSA C22.2 No. 60950-1, UL 61010-2-201
<b>standards, specifications, approvals / hazardous environments</b>	
certificate of suitability	
• ATEX	Yes
• UKEX	Yes
• IECEx	Yes
• ULhazloc approval	Yes

<ul style="list-style-type: none"> <li>• CCC / for hazardous zone according to GB standard</li> <li>• FM registration</li> </ul>	<p>Yes</p> <p>Yes</p>				
<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>• RoHS conformity</li> </ul>	<p>No</p> <p>Yes</p>				
resistance to air pollution / conformity according to ANSI/ISA-71.04	Yes; G3				
IT security for industrial automation systems / according to IEC 62443-4-2:2019	Yes				
<b>standards, specifications, approvals / Environmental Product Declaration</b>					
Environmental Product Declaration	Yes				
global warming potential [CO2 eq] <ul style="list-style-type: none"> <li>• total</li> <li>• during manufacturing</li> <li>• during operation</li> <li>• after end of life</li> </ul>	<p>306.92 kg</p> <p>109.07 kg</p> <p>197.3 kg</p> <p>0.55 kg</p>				
<b>product functions / general</b>					
MTBF	56 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>	<p><a href="https://support.industry.siemens.com/cs/ww/en/view/109766358">https://support.industry.siemens.com/cs/ww/en/view/109766358</a></p> <p><a href="https://www.siemens.com/tstcloud">https://www.siemens.com/tstcloud</a></p> <p><a href="https://www.siemens.com/simatic-net">https://www.siemens.com/simatic-net</a></p> <p><a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a></p> <p><a href="https://www.automation.siemens.com/bilddb">https://www.automation.siemens.com/bilddb</a></p> <p><a href="https://www.siemens.com/cax">https://www.siemens.com/cax</a></p> <p><a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a></p>				
<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>				
<b>Approvals / Certificates</b>					
<b>General Product Approval</b>					
 EG-Konf.	<a href="#">Declaration of Conformity</a>		<a href="#">China RoHS</a>	 UL	<a href="#">Declaration of Conformity</a>
<b>General Product Approval</b>		<b>EMV</b>	<b>For use in hazardous locations</b>		
 RCM	<a href="#">TUEV</a>	<a href="#">KC</a>	 IECEx	 ATEX	<a href="#">FM</a>

For use in hazardous locations	Test Certificates	Environment	Industrial Communication
--------------------------------	-------------------	-------------	--------------------------

[CCC-Ex](#)

[Type Test Certificates/Test Report](#)



[PROFINET](#)

---

last modified:

10/30/2025