



SCALANCE XB216 managed Layer 2 IE switch, 16X 10/100 Mbit/s RJ45 ports, 1x console port, diagnostics LED redundant power supply IEC 62443-4-2 certified; temperature range 0 °C to +60 °C; DIN-rail mounting, PROFINET IO device Ethernet/IP certificate, default PROFINET.

<b>product type designation</b>	<b>SCALANCE XB216</b>
<b>transfer rate</b>	
transfer rate	10 Mbit/s, 100 Mbit/s
number of ports / maximum	16
<b>interfaces / for communication / maximum configuration for modular devices</b>	
number of electrical ports / maximum	16
<b>interfaces / for communication / integrated</b>	
number of electrical connections	
• for network components or terminal equipment	16; RJ45
<b>interfaces / other</b>	
number of electrical connections	
• for operator console	1
• for management purposes	1
• for power supply	1
type of electrical connection	
• for operator console	RJ11
• for management purposes	RJ45
<b>supply voltage, current consumption, power loss</b>	
product component / connection for redundant voltage supply	Yes
<b>type of voltage / 1 / of the supply voltage</b>	DC
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	6.7 W
• supply voltage / 1 / rated value	19.2 ... 28.8 V
• consumed current / 1 / maximum	0.28 A
• type of electrical connection / 1 / for power supply	6-pole terminal block
• product component / 1 / fusing at power supply input	Yes
<b>ambient conditions</b>	
ambient temperature	
• during operation	0 ... 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
<b>design, dimensions and weights</b>	
design	compact
width	80 mm
height	117 mm
depth	109 mm

net weight	0.4 kg
material / of the enclosure	Polycarbonate (PC-GF10)
fastening method	Yes
• 35 mm top hat DIN rail mounting	Yes
<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	
• CLI	Yes
• web-based management	Yes
• MIB support	Yes
• TRAPs via email	Yes
• configuration with STEP 7	Yes
• RMON	Yes
• port mirroring	Yes
• multiport mirroring	No
• CoS	Yes
• PROFINET IO diagnosis	Yes
PROFINET conformity class	B
network load class / according to PROFINET	3
product function / switch-managed	Yes
telegram length / for Ethernet / maximum	1632 byte
protocol / is supported	
• Telnet	Yes
• HTTP	Yes
• HTTPS	Yes
• TFTP	Yes
• FTP	Yes
• DCP	Yes
• LLDP	Yes
• EtherNet/IP	Yes
• SNMP v1	Yes
• SNMP v2	Yes
• SNMP v3	Yes
• IGMP (snooping/querier)	Yes
identification & maintenance function	
• I&M0 - device-specific information	Yes
• I&M1 - higher level designation/location designation	Yes
<b>product functions / diagnostics</b>	
product function	
• port diagnostics	Yes
• statistics Packet Size	Yes
• statistics packet type	Yes
• error statistics	Yes
• SysLog	Yes
• loopback diagnostics	Yes
<b>product functions / VLAN</b>	
product function	
• VLAN - port based	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
<b>product functions / redundancy</b>	
product function	
• ring redundancy	Yes

<ul style="list-style-type: none"> <li>• High Speed Redundancy Protocol (HRP)</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• high speed redundancy protocol (HRP) with redundancy manager</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• high speed redundancy protocol (HRP) with standby redundancy</li> </ul>	Yes
protocol / is supported / Media Redundancy Protocol (MRP)	Yes
product function	
<ul style="list-style-type: none"> <li>• media redundancy protocol (MRP) with redundancy manager</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Media Redundancy Protocol Interconnection (MRP-I)</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• redundancy procedure STP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• redundancy procedure RSTP</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• redundancy procedure RSTP+</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Parallel Redundancy Protocol (PRP)/operation in the PRP-network</li> </ul>	No
<ul style="list-style-type: none"> <li>• passive listening</li> </ul>	Yes
protocol / is supported	
<ul style="list-style-type: none"> <li>• LACP</li> </ul>	Yes
<b>product functions / security</b>	
product function	
<ul style="list-style-type: none"> <li>• ACL - MAC-based</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• ACL - port/MAC-based</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• IEEE 802.1x (radius)</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• broadcast/multicast/unicast limiter</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• broadcast blocking</li> </ul>	Yes
protocol / is supported	
<ul style="list-style-type: none"> <li>• SSH</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• SSL</li> </ul>	Yes
<b>product functions / time</b>	
product function	
<ul style="list-style-type: none"> <li>• SICLOCK support</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• NTP-client</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• SNTP client</li> </ul>	Yes
protocol / is supported	
<ul style="list-style-type: none"> <li>• SNTP</li> </ul>	Yes
<b>standards, specifications, approvals</b>	
standard	
<ul style="list-style-type: none"> <li>• for FM</li> </ul>	FM3611: Class 1, Division 2, Group A, B, C, D / T4, CL.1, Zone 2, GP. IIC, T4, FM19US0167X
<ul style="list-style-type: none"> <li>• for emitted interference</li> </ul>	EN 61000-6-4 (Class A)
<ul style="list-style-type: none"> <li>• for interference immunity</li> </ul>	EN 61000-6-2
IT security for industrial automation systems / according to IEC 62443-4-2:2019	Yes
MTBF	60 a
reference code	
<ul style="list-style-type: none"> <li>• according to IEC 81346-2</li> </ul>	KF
<ul style="list-style-type: none"> <li>• according to IEC 81346-2:2019</li> </ul>	KFE
<b>standards, specifications, approvals / CE</b>	
certificate of suitability / CE marking	Yes
certificate of suitability / RoHS conformity	Yes; 2011/65/EU
<b>standards, specifications, approvals / hazardous environments</b>	
standard / for hazardous zone	EN 60079-0 : 2006, EN 60079-15: 2005, II 3 G Ex nA II T4 KEMA 07 ATEX 0145X
<ul style="list-style-type: none"> <li>• from CSA and UL</li> </ul>	ANSI / ISA 12.12.01, CSA C22.2 No. 213-M1987, CL. 1 / Div. 2 / GP. A, B, C, D T4, CL. 1 / Zone 2 / GP. IIC, T8, E240480
certificate of suitability	
<ul style="list-style-type: none"> <li>• CCC / for hazardous zone according to GB standard</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• CCC / for hazardous zone according to GB standard / as marking</li> </ul>	Ex nA IIC T4 Gc
<b>standards, specifications, approvals / other</b>	
certificate of suitability	EN 61000-6-2, EN 61000-6-4
<ul style="list-style-type: none"> <li>• C-Tick</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• KC approval</li> </ul>	Yes

## further information / internet links

### internet link

- to web page: selection aid TIA Selection Tool
- to website: Industrial communication
- to website: Industry Mall
- to website: Information and Download Center
- to website: Image database
- to website: CAx-Download-Manager
- to website: Industry Online Support

<http://www.siemens.com/tia-selection-tool>  
<http://www.siemens.com/simatic-net>  
<https://mall.industry.siemens.com>  
<http://www.siemens.com/industry/infocenter>  
<http://automation.siemens.com/bilddb>  
<http://www.siemens.com/cax>  
<https://support.industry.siemens.com>

## security information

### security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>. 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 Security RSS Feed under <https://www.siemens.com/cert>. (V4.6)

### last modified:

9/22/2023 