SIEMENS

Data sheet



SCALANCE XC116, Unmanaged IE switch, 16x 10/100 Mbit/s RJ45 ports, LED diagnostics, error-signaling contact with set pushbutton, redundant power supply Manual available as a download.

product type designation	SCALANCE XC116		
transfer rate			
transfer rate	10 Mbit/s, 100 Mbit/s		
interfaces / for communication / maximum configuration for modular devices			
number of electrical ports / maximum	16		
interfaces / for communication / integrated			
number of electrical connections			
 for network components or terminal equipment 	16; RJ45		
interfaces / other			
number of electrical connections			
 for signaling contact 	1		
• for power supply	1		
type of electrical connection			
 for signaling contact 	2-pole terminal block		
for power supply	4-pole terminal block		
signal inputs/outputs			
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		
type of voltage / 1 / of the supply voltage	DC		
supply voltage / 1 / rated value	24 V		
power loss [W] / 1 / rated value	5.4 W		
 consumed current / 1 / at rated supply voltage / maximum 	0.45 A		
supply voltage / 1 / rated value	9.6 31.2 V		
 type of electrical connection / 1 / for power supply 	4-pole terminal block		
 product component / 1 / fusing at power supply input 	Yes		
fuse protection type / 1 / at input for supply voltage	2.5 A / 125 V		
ambient conditions			
ambient temperature			
during operation	-40 +70 °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	IP20		
design, dimensions and weights			

design compact width 120 mm height 147 mm depth 125 mm	
height 147 mm depth 125 mm	
depth 125 mm	
1717	
not words	
net weight 0.775 kg material / of the enclosure Polycarbonate (PC-GF10)	
fastening method • 35 mm top hat DIN rail mounting Yes	
3	
3	
S7-1500 rail mounting Yes product features, product functions, product components / general	
number of automatically learnable MAC addresses 2048	
product functions / management, configuration, engineering	
product function	
• multiport mirroring No	
• CoS Yes	
product function / switch-managed No	
product function	
• is supported / identification link Yes	
product functions / redundancy	
product function	
 Parallel Redundancy Protocol (PRP)/operation in the PRP-network 	
Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA)	
standards, specifications, approvals	
standard	
• for safety / from CSA and UL UL 60950-1, CSA C22.2 No. 60950-1	
• for emitted interference EN 61000-6-4 (Class B)	
reference code	
• according to IEC 81346-2 KF	
• according to IEC 81346-2:2019 KFE	
standards, specifications, approvals / CE	
certificate of suitability / CE marking Yes	
standards, specifications, approvals / hazardous environments	
standard / for hazardous zone EN 60079-0:2012 + A11:2013, EN60079 KEMA 07ATEX0145 X, IEC 6079-0:2011	1, IEC 6079-0-15:2010
• from CSA and UL UL 1604 and UL 2279-15 (Hazardous Lo B, C, D / T, Class 1 / Zone 2 / Group IIC	
certificate of suitability	
CCC / for hazardous zone according to GB standard Yes	
CCC / for hazardous zone according to GB standard / as marking Ex nA IIC T4 Gc	
standards, specifications, approvals / other	
laser protection class LED Class 1	
certificate of suitability EN 61000-6-2, EN 61000-6-4	
• C-Tick Yes	
• KC approval Yes	
• E1 approval	
 E1 approval EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 Yes	
• EC Declaration of Conformity EN 61010, IEC 61010-1, Yes	
• EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 standards, specifications, approvals / marine classification Yes	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 Standards, specifications, approvals / marine classification Marine classification association	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 standards, specifications, approvals / marine classification Marine classification association American Bureau of Shipping Europe Ltd. (ABS) Yes	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 Standards, specifications, approvals / marine classification Marine classification association American Bureau of Shipping Europe Ltd. (ABS) French marine classification society (BV) Yes	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 Standards, specifications, approvals / marine classification Marine classification association American Bureau of Shipping Europe Ltd. (ABS) French marine classification society (BV) Det Norske Veritas (DNV) No	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 Standards, specifications, approvals / marine classification Marine classification association American Bureau of Shipping Europe Ltd. (ABS) French marine classification society (BV) Det Norske Veritas (DNV) Germanische Lloyd (GL) No	
EC Declaration of Conformity EN 61010, IEC 61010-1, UL 61010A-1 Standards, specifications, approvals / marine classification Marine classification association American Bureau of Shipping Europe Ltd. (ABS) French marine classification society (BV) Det Norske Veritas (DNV) Germanische Lloyd (GL) DNV GL Yes	

Environmental Product Declaration Yes Global Warming Potential [CO2 eq] / total Global Warming Potential [CO2 eq] / during manufacturing Global Warming Potential [CO2 eq] / during operation global warming potential [CO2 eq] / during operation global warming potential [CO2 eq] / after end of life 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: Image database to website: Image database to website: CAx-Download-Manager to website: Total t	standards, specifications, approvals / Environmental Product Declaration			
Global Warming Potential [CO2 eq] / during manufacturing Global Warming Potential [CO2 eq] / during operation global warming potential [CO2 eq] / after end of life outper information / internet link Internet link to web page: selection aid TIA Selection Tool to website: Industry Mall to website: Industry Mall to website: Industry Mall to website: Information and Download Center to website: Information and Download Center to website: Industry Mall to website: Industry Online Support thttp://www.siemens.com/foldstb http://www.siemens.com/foldstb http://www.siemens.com/foldstb http://www.siemens.com/sax thttps://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 one, Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions undergo continuously maintain – a holistic, state-of-the-art industrial security measures are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks. Such systems, machines and networks Such systems, machines and components should only be connected to an enterprise network or the interne	Environmental Product Declaration	Yes		
Global Warming Potential [CO2 eq] / during manufacturing Global Warming Potential [CO2 eq] / during operation global warming potential [CO2 eq] / after end of life outper information / internet link Internet link to web page: selection aid TIA Selection Tool to website: Industry Mall to website: Industry Mall to website: Industry Mall to website: Information and Download Center to website: Information and Download Center to website: Industry Mall to website: Industry Online Support thttp://www.siemens.com/foldstb http://www.siemens.com/foldstb http://www.siemens.com/foldstb http://www.siemens.com/sax thttps://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 one, Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions constitute one element of such a concept. Siemen's products and solutions undergo continuously maintain – a holistic, state-of-the-art industrial security measures are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks. Such systems, machines and networks Such systems, machines and components should only be connected to an enterprise network or the interne				
### Global Warning Potential [CO2 eq] / after end of life 0.57 kg ### further information / internet links **Internet link*	Global Warming Potential [CO2 eq] / total	441.	1 kg	
global warming potential [CO2 eq] / after end of life further information / internet links internet link		47.6	7 kg	
internet link intern	 Global Warming Potential [CO2 eq] / during 	operation 392.	82 kg	
intermet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industry Mall • to website: Industry Mall • to website: Information and Download Center • to website: Information and Download Center • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industry Online Support **Ecurity information **Security information information information information information information in information info	 global warming potential [CO2 eq] / after end 	of life 0.57	kg	
to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Industry Mall to website: Information and Download Center to website: Information and Download Center to website: Image database to website: CAx-Download-Manager to website: Industry Online Support to website: Industry Online Support security information Security information of plants, systems, machines and networks against cyber threats, it is necessary to implement and continuously maintain — a holistic, state-of-the-art industrial security functions that are not information on industrial security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be inplemented, please visit https://www.siemens.com/industrialsecurity. Siemens' products and solutions undergo continuous	further information / internet links			
to website: Industry Mall to website: Information and Download Center to website: Image database to website: CAx-Download-Manager to website: Industry Online Support to website: Industry Online Support 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 well on the tent 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.	internet link			
to website: Industry Mall to website: Information and Download Center to website: Image database to website: CAx-Download-Manager to website: CAx-Download-Manager to website: Industry Online Support security information Security information Security information Security information Silemens 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)	 to web page: selection aid TIA Selection Too 	l <u>http:</u>	//www.siemens.com/tia-selection-tool	
to website: Information and Download Center to website: Image database to website: CAx-Download-Manager to website: Industry Online Support security information security information 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) Approvals / Certificates	 to website: Industrial communication 	http:	//www.siemens.com/simatic-net	
* to website: Image database * to website: CAx-Download-Manager * to website: Industry Online Support **security information **security information **Security information **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) **Approvals / Certificates**	 to website: Industry Mall 	https	s://mall.industry.siemens.com	
* to website: CAx-Download-Manager * to website: Industry Online Support *** *** to website: Industry Online Support *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ** ** *** *** *** *** *** *** *** *** *** ** ** ** **	 to website: Information and Download Cente 	r <u>http:</u>	//www.siemens.com/industry/infocenter	
• to website: Industry Online Support https://support.industry.siemens.com 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) Approvals / Certificates	 to website: Image database 	http:	//automation.siemens.com/bilddb	
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)	to website: CAx-Download-Manager	http:	//www.siemens.com/cax	
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)	• to website: Industry Online Support	https	s://support.industry.siemens.com	
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)	security information			
			ort the secure operation of plants, systems, machines and networks. In r to protect plants, systems, machines and networks against cyber threats, necessary to implement – and continuously maintain – a holistic, state-of-art industrial security concept. Siemens' products and solutions constitute element of such a concept. Customers are responsible for preventing atthorized access to their plants, systems, machines and networks. Such ems, machines and components should only be connected to an enterprise rork or the internet if and to the extent such a connection is necessary and when appropriate security measures (e.g. firewalls and/or network mentation) are in place. For additional information on industrial security sures that may be implemented, please visit strongly mmends that product updates are applied as soon as they are available that the latest product versions are used. Use of product versions that are onger supported, and failure to apply the latest updates may increase ormer's exposure to cyber threats. To stay informed about product updates, acribe to the Siemens Industrial Security RSS Feed under	
General Product Approval EMC For use in hazardous locations	Approvals / Certificates			
	General Product Approval	EMC	For use in hazardous locations	

Manufacturer Declaration





ATEX-Zone 2-Declaration



<u>FM</u>

For use in hazardous locations

Declaration of Conformity

Marine / Shipping

CCC-Ex







Manufacturer Declaration



Marine / Shipping





NK / Nippon Kaiji Kyokai







Marine / Shipping

other

Environment



Manufacturer Declaration



last modified: 10/27/2023 🖸