



-- spare part -- SCALANCE X204IRT PRO, managed IE IRT switch with degree of protection IP65/67, 4x 10/100 Mbps push-pull RJ45 ports, error signaling contact with set pushbutton; power supply (load/encoder); PROFINET IO device, network management, redundancy manager integrated, including electronic manual on CD-ROM, C-PLUG optional.

product type designation	
product brand name	SCALANCE
product type designation	X204IRT PRO
transfer rate	
transfer rate	10 Mbit/s, 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
type of electrical connection	
• for signaling contact	5-pin M12 socket
• for power supply	5-pin push-pull plug PRO socket
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	
type of voltage / 1 / of the supply voltage	DC
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	4.8 W
• supply voltage / 1 / rated value	18 ... 32 V
• consumed current / 1 / maximum	0.2 A
• type of electrical connection / 1 / for power supply	5-pin Push Pull Plug PRO socket
• product component / 1 / fusing at power supply input	Yes
• fuse protection type / 1 / at input for supply voltage	0.6 A / 60 V
ambient conditions	
ambient temperature	
• during operation	-25 ... +70 °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	IP65
design, dimensions and weights	

design	compact
width	90 mm
height	125 mm
depth	124 mm
net weight	1 kg
fastening method	
• 35 mm top hat DIN rail mounting	Yes
• wall mounting	Yes
• S7-300 rail mounting	Yes
• S7-1500 rail mounting	No
product features, product functions, product components / general	
cascading in the case of a redundant ring / at reconfiguration time of $\leq 0.3\text{ s}$	100
cascading in cases of star topology	any (depending only on signal propagation time)
product functions / management, configuration, engineering	
product function	
• CLI	Yes
• web-based management	Yes
• MIB support	Yes
• TRAPs via email	Yes
• configuration with STEP 7	Yes
• port mirroring	No
• multipoint mirroring	No
• with IRT / PROFINET IO switch	Yes
• PROFINET IO diagnosis	Yes
• switch-managed	Yes
PROFINET conformity class	C
network load class / according to PROFINET	2
protocol / is supported	
• Telnet	Yes
• HTTP	Yes
• HTTPS	Yes
• TFTP	Yes
• FTP	Yes
• BOOTP	No
• DCP	Yes
• LLDP	Yes
• SNMP v1	Yes
• SNMP v2	Yes
• SNMP v3	Yes
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 / DHCP	
product function	
• DHCP client	Yes
product functions / redundancy	
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

<ul style="list-style-type: none"> • Parallel Redundancy Protocol (PRP)/operation in the PRP-network 	Yes
<ul style="list-style-type: none"> • Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA) 	No
<ul style="list-style-type: none"> • passive listening 	Yes
product functions / security	
protocol / is supported	
<ul style="list-style-type: none"> • SSH 	Yes
product functions / time	
product function	
<ul style="list-style-type: none"> • SICLOCK support 	Yes
protocol / is supported	
<ul style="list-style-type: none"> • NTP • SNTP 	No Yes
standards, specifications, approvals	
certificate of suitability	
<ul style="list-style-type: none"> • CE marking • KC approval 	Yes Yes
standard	
<ul style="list-style-type: none"> • for safety / from CSA and UL 	UL 60950-1 E115352, CSA C22.2 No. 60950-1
standards, specifications, approvals / hazardous environments	
certificate of suitability	
<ul style="list-style-type: none"> • CCC / for hazardous zone according to GB standard 	Yes
standards, specifications, approvals / other	
certificate of suitability	
<ul style="list-style-type: none"> • railway application in accordance with EN 50155 • railway application in accordance with EN 50124-1 	No No
standards, specifications, approvals / marine classification	
Marine classification association	
<ul style="list-style-type: none"> • American Bureau of Shipping Europe Ltd. (ABS) • French marine classification society (BV) • DNV GL • Lloyds Register of Shipping (LRS) • Nippon Kaiji Kyokai (NK) • Polski Rejestr Statkow (PRS) • Royal Institution of Naval Architects (RINA) 	Yes Yes Yes Yes Yes Yes Yes
product functions / general	
MTBF	98.55 a
reference code	
<ul style="list-style-type: none"> • according to IEC 81346-2 • according to IEC 81346-2:2019 	KF KFE
further information / internet links	
internet link	
<ul style="list-style-type: none"> • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support 	https://support.industry.siemens.com/cs/ww/de/view/109766358 https://www.siemens.com/tstcloud https://www.siemens.com/simatic-net https://www.automation.siemens.com/bilddb https://www.siemens.com/cax 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 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

General Product Approval



[Declaration of Conformity](#)



General Product Approval

For use in hazardous locations

[Miscellaneous](#)



[EM](#)

[CCC-Ex](#)

Marine / Shipping



[NK / Nippon Kaiji Kyokai](#)



Marine / Shipping

Environment

Industrial Communication



[Confirmation](#)



[PROFINET](#)

last modified:

10/23/2024 